Modular Representation Theory of Algebraic Groups and Their Lie Algebras

by

Matthew Westaway

Thesis

Submitted to the University of Warwick

for the degree of

Doctor of Philosophy in Mathematics

Mathematics Institute

March 2020

Contents

List of Tables

Acknowledgments

The following thesis would not have been possible without the support and assistance of my PhD supervisors Dmitriy Rumynin and Inna Capdeboscq. I would also like to thank them for suggesting these (and other) topics for me to study, and to thank Dmitriy for his co-authorship with me of the two papers which make up Chapters 5 and 6. More generally, I wish to extend my thanks to the whole of the University of Warwick for providing a great environment in which to undertake my postgraduate study.

Furthermore, I would like to thank Lewis Topley for some useful conversations regarding the material in this thesis, as well as for giving me the opportunity to present some of this research at the University of Kent. Similarly, I want to thank Alexander Premet and Simon Goodwin for allowing me to talk about my research at the University of Manchester and the University of Birmingham. My thanks also go out to the various referees of the papers which make up these thesis, many of whom have made valuable comments which led to changes in the papers. Thanks also go to Ami Braun, Jim Humphreys and Stephen Donkin for valuable discussions about the content of Chapters 5 and 6 with my coauthor for those papers. I would also like to thank the examiners of this thesis, Alexander Premet and Adam Thomas, for their useful comments and corrections.

Finally, I greatly want to thank my parents for supporting me during my postgraduate study and in everything else I do.

Declarations

This thesis is being submitted for the degree of Doctor of Philosophy in Mathematics. This PhD was undertaken at the University of Warwick and was funded by a studentship from the Engineering and Physical Sciences Research Council.

The original work in this thesis is entirely contained in the following four papers: [Westaway, 2018], [Westaway, 2019], [Rumynin and Westaway, 2018], and [Rumynin and Westaway, 2019]. The former two papers were completed solely by the author, except at points explicitly indicated in the text. The latter two papers were completed jointly with my PhD supervisor, Dmitriy Rumynin. The paper [Rumynin and Westaway, 2019] has been published in the Pacific Journal of Mathematics. The paper [Westaway, 2018] has been accepted for publication by the Journal of the Mathematical Society of Japan. The paper [Westaway, 2019] has been accepted for publication by the Nagoya Mathematical Journal. The remaining paper is currently under review at a journal.

Abstract

Each affine algebraic group G over an algebraically closed field $\mathbb{K}$ of positive characteristic comes equipped with a Frobenius morphism, which corresponds to the p-th power map on the associated coordinate algebra. The kernel G_1 of this morphism is called the first Frobenius kernel and is a normal subgroup scheme of G. Its representation theory is precisely the restricted representation theory of $\mathfrak{g}$, the Lie algebra of G.

This correspondence comes from an isomorphism between the restricted enveloping algebra of $\mathfrak{g}$ and the distribution algebra of G_1; the former is a central quotient of $U(\mathfrak{g})$, while the latter is a Hopf subalgebra of the distribution algebra of G – a Hopf algebra closely related to the representation theory of G. By deforming the restricted enveloping algebra of $\mathfrak{g}$ we obtain the reduced enveloping algebras $U_\chi(\mathfrak{g})$. Every irreducible $\mathfrak{g}$-module is an irreducible $U_\chi(\mathfrak{g})$-module for some $\chi \in \mathfrak{g}^*$.

The first question tackled by this thesis is whether a similar deformation theory can be developed for the higher Frobenius kernels G_r of G, obtained by composing F with itself multiple times. We find that it can, and exhibit a number of structural results about the corresponding algebras, as well as proving many results about their representations.

The second question considered here is when a restricted representation of $\mathfrak{g}$ can be integrated to G. This can easily be rephrased as a question about extending representations from G_1 to G. Two approaches to this problem are taken. The first uses stability and obtains an algorithm placing cohomological conditions on a positive answer to this question. The second uses exponentials, and affirmatively answers the question for a certain type of representation which we call over-restricted.

Chapter 1

Introduction

Let G be an algebraic group. This is a mathematical object which lies in the intersection of two fields of study: it is a variety, placing it in the field of algebraic geometry, but it also satisfies the axioms for a group, giving it a home within the study of group theory. Both algebraic geometry and group theory employ in their study an idea which has been in use for hundreds of years. This idea is quite simple: linear objects are straightforward to understand, so the more linear one can make a complicated object, the easier it is to comprehend. Within algebraic geometry, this idea appears in the form of tangent spaces; within group theory, in representations. When trying to employ this idea for algebraic groups, therefore, we have multiple avenues to explore.

More explicitly, the tangent space of G at the identity has the structure of a Lie algebra - we call it $\mathfrak{g}$. As indicated above, we would like to understand the relationship between G and $\mathfrak{g}$, and we would like to understand the representation theory of G. Combining these two goals, we may sensibly ask the question: how closely related are the representation theories of G and $\mathfrak{g}$?

The algebraic group G is defined over an algebraically closed field $\mathbb{K}$. As in other areas of study, the characteristic of $\mathbb{K}$ plays an important role in how we develop answers to this question. When the characteristic of $\mathbb{K}$ is zero, many results are known - some of these will be surveyed below. In prime characteristic, however, the existing record is less extensive.

One key difference between the cases of zero and non-zero characteristic is the role of the universal enveloping algebra of $\mathfrak{g}$, which we denote $U(\mathfrak{g})$. In positive characteristic, one has to distinguish between $U(\mathfrak{g})$, which is only defined from the Lie algebra, and the distribution algebra $\mathrm{Dist}(G)$, whose elements are linear maps $\delta : \mathbb{K}[G] \to \mathbb{K}$ satisfying an additional property. Both contain $\mathfrak{g}$ as a Lie subalgebra, and a G-module can be easily given the structure of a module over either of these algebras. In characteristic zero $U(\mathfrak{g})$ and $\mathrm{Dist}(G)$ coincide, but in characteristic $p > 0$ they are different objects. The representation theory of $\mathfrak{g}$ is closely related (in fact, identical to) the representation theory of $U(\mathfrak{g})$, but the representation theory of G is better captured by the representation theory of $\mathrm{Dist}(G)$.

As a result, understanding representations of an algebraic group and its Lie algebra requires the study of both the universal enveloping algebra and the distribution algebra, as well as the connection between the two. The connection largely stems from the isomorphism

$$U_0(\mathfrak{g}) \cong \mathrm{Dist}(G_1), \tag{1.1}$$

where $U_0(\mathfrak{g})$ is a quotient of $U(\mathfrak{g})$ and $\mathrm{Dist}(G_1)$ is a Hopf subalgebra of $\mathrm{Dist}(G)$. This connection is somehow the starting point of this thesis, and it is from this common groundwork that the thesis breaks into two halves.

A Question of Friedlander and Parshall

In 1988 and 1990, Eric Friedlander and Brian Parshall published a pair of papers[1] exploring the modular representation theory of Lie algebras. They obtained a number of important results on this topic and at the end of their 1990 paper they posed several questions for further study. One of these, numbered (5.4), asked the following:

> ``Do the [reduced enveloping algebras $U_\chi(\mathfrak{g})$] have natural analogues corresponding to the infinitesimal group schemes G_r [the higher Frobenius kernels] associated to G [an algebraic group over an algebraically closed field of positive characteristic] for $r > 1$?''[2]

Let us briefly recall the background to this question. Given a linear form $\chi \in \mathfrak{g}^*$, we define the *reduced enveloping algebra*

$$U_\chi(\mathfrak{g}) := \frac{U(\mathfrak{g})}{\langle x^p - x^{[p]} - \chi(x)^p \mid x \in \mathfrak{g} \rangle},$$

where $x \mapsto x^{[p]}$ is the p-th power map with which the restricted Lie algebra $\mathfrak{g}$ is equipped. The reduced enveloping algebras are important for a reason: every irreducible $\mathfrak{g}$-module is an irreducible $U_\chi(\mathfrak{g})$-module for some $\chi \in \mathfrak{g}^*$. As a result, understanding the $U_\chi(\mathfrak{g})$ is key to understanding the irreducible representations of $\mathfrak{g}$.[3]

When $\chi = 0$, we precisely obtain the algebra $U_0(\mathfrak{g})$ mentioned earlier, called the *restricted enveloping algebra* of $\mathfrak{g}$. Using the isomorphism in (1.1) we may hence describe the reduced enveloping algebras $U_\chi(\mathfrak{g})$ as *deformations* of $\mathrm{Dist}(G_1)$.

What is $\mathrm{Dist}(G_1)$? This is simply the distribution algebra of the infinitesimal group scheme G_1, the *first Frobenius kernel* of G. The first Frobenius kernel is obtained as the kernel of some homomorphism $F : G \to G$, so we may iterate the map

[1] [Friedlander and Parshall, 1988] and [Friedlander and Parshall, 1990].
[2] See [Friedlander and Parshall, 1990].
[3] This fundamental observation can be found most notably in [Kac and Weisfeiler, 1971].

to obtain the *higher Frobenius kernels* G_r of G. This bring us back to Friedlander and Parshall's question, which ultimately asks whether similar deformations exist for $\mathrm{Dist}(G_r)$ with $r > 1$.

To answer this question, we must first define and study a family of higher universal enveloping algebras $U^{[r]}(G)$ for $r \in \mathbb{N}$, analogues of the universal enveloping algebra in these higher cases. When $r = 0$, this algebra is precisely $U(\mathfrak{g})$, and the family of algebras $\{U^{[r]}(G)\}_{r\in\mathbb{N}}$ form a direct system with limit $\mathrm{Dist}(G)$. This family of algebras was first introduced in [Kaneda and Ye, 2007], however their study of it was related primarily to its connection to the study of arithmetic differential operators.[4] The sum and substance of their results on the structure of this algebra can be found in Subsection 3.1.1 of this thesis, and this algebra has been minimally studied since then. Indeed, Kaneda and Ye's construction is not especially useful for the goals of this thesis and we define the algebra $U^{[r]}(G)$ in a different way, before showing that these constructions are isomorphic in Subsection 3.4.2.

The higher universal enveloping algebras $U^{[r]}(G)$ share many similarities with the universal enveloping algebras. They are finitely generated over their centres (Proposition 3.4.1.1), all of their irreducible modules are finite-dimensional (Theorem 3.4.1.2), and they have a Poincaré-Birkhoff-Witt basis (Corollary 3.3.1.8 and Proposition 3.3.2.2). In fact, there exist surjective Hopf algebra homomorphisms $U^{[r]}(G) \to U(\mathfrak{g})^{(r)}$ for each $r \in \mathbb{N}$ by Proposition 3.2.2.1 and Corollary 3.2.2.3.[5] Furthermore, Lemma 3.3.1.1 enables us to define a notion of p-th powers in these algebras, and hence to define the algebras $U_\chi^{[r]}(G)$ indexed by $\chi \in \mathfrak{g}^*$. These $U_\chi^{[r]}(G)$ are the analogues of the $U_\chi(\mathfrak{g})$ in this higher setting, and every irreducible $U^{[r]}(G)$-module is an irreducible $U_\chi^{[r]}(G)$-module for some $\chi \in \mathfrak{g}^*$ (Proposition 3.5.1.2).

In Chapter 4 we restrict to the case of reductive groups and show, considering here irreducible modules only up to isomorphism, that there is a well-defined bijection,[6]

$$\Psi_\chi : \mathrm{Irr}(U_\chi^{[r]}(G)) \xrightarrow{\sim} \mathrm{Irr}(\mathrm{Dist}(G_r)) \times \mathrm{Irr}(U_\chi(\mathfrak{g})).$$

When $\chi = 0$, we recover Steinberg's tensor product theorem by iterating this process. More generally, the bijection allows us to derive various structural results about the irreducible $U_\chi^{[r]}(G)$-modules. In particular, given an irreducible $\mathrm{Dist}(G_r)$-module P one can construct teenage Verma modules $Z_\chi^r(P, \lambda)$ which behave as the baby Verma modules $Z_\chi(\lambda)$ do in the $r = 0$ case (Proposition 4.1.3.4). This allows us to classify all irreducible $U_\chi^{[r]}(G)$-modules when χ is regular in Theorem 4.1.4.1. The main techniques which allow us to prove these results come from the work of Schneider and Witherspoon on Clifford theory for Hopf algebras.

[4] See [Berthelot, 1996] for more discussion of arithmetic differential operators.
[5] Here, $U(\mathfrak{g})^{(r)}$ indicates the ring $U(\mathfrak{g})$ with a twisted $\mathbb{K}$-algebra structure.
[6] See Theorem 4.1.2.3 and Corollary 4.1.2.6.

The Humphreys-Verma Conjecture

Turning now to the second half of this thesis, we wish to examine when representations can be integrated from a Lie algebra to the associated algebraic group. To begin this discussion, suppose for the moment that G is a simply-connected matrix Lie group over the complex numbers $\mathbb{C}$, with Lie algebra $\mathfrak{g}$. Given a finite-dimensional representation $\theta : \mathfrak{g} \to \mathfrak{gl}(V)$, it is well known that there exists a unique Lie group homomorphism $\Theta : G \to \mathrm{GL}(V)$ such that $d\Theta = \theta$.[7] In other words, there is a one-to-one correspondence between finite-dimensional representations of $\mathfrak{g}$ and of G. Specifically, every element of G can be written as $e^{x_1} \dots e^{x_n}$ for some $x_1, \dots, x_n \in \mathfrak{g}$. Defining

$$\Theta(e^{x_1} \dots e^{x_n}) = e^{\theta(x_1)} \dots e^{\theta(x_n)}$$

turns out to yield a representation of G.

A similar technique can be used to show that, if G is a semisimple simply-connected algebraic group over a field of characteristic zero with semisimple Lie algebra $\mathfrak{g}$, then G and $\mathfrak{g}$ also have the same representations. This can also be seen from the fact that the category of representations of $\mathfrak{g}$ is a Tannakian category, with G the associated affine algebraic group.[8]

In positive characteristic $p > 0$, however, things are more complicated. Firstly, the only representations of $\mathfrak{g}$ which can be obtained from G are the *restricted representations* of $\mathfrak{g}$, i.e. those that preserve the p-structure. So, at a minimum, we have to limit ourselves to consideration of restricted representations.

A second obstacle to understanding such a correspondence in positive characteristic is the difference between irreducible and indecomposable representations. Let us restrict our attention to a semisimple, simply connected algebraic group G over an algebraically closed field $\mathbb{K}$ of characteristic $p > 0$, and let $\mathfrak{g}$ be its Lie algebra. Using the isomorphism in (1.1), restricted representations of $\mathfrak{g}$ are precisely representations of the first Frobenius kernel G_1 of G. We are able to classify the irreducible representations of G and of G_r for all $r \geqslant 1$, and it is then straightforward to see that every irreducible restricted representation of $\mathfrak{g}$ extends to an irreducible representation of G. The earliest proof of this result lies in [Curtis, 1960], but the reader can also find a more in depth discussion in Chapters II.2 and II.3 of [Jantzen, 1987].

On the other hand, our understanding of the question for indecomposable representations is a lot less complete. The following conjecture was made by Humphreys and Verma,[9] and has become known as the *Humphreys-Verma Conjecture*:

Conjecture (Humphreys-Verma conjecture)**.** *Let G be a semisimple, simply-connected algebraic group over an algebraically closed field $\mathbb{K}$ of positive characteristic $p > 0$.*

[7] See, for example, Theorem 5.6 in [Hall, 2015].
[8] See, for example, [Milne, 2017].
[9] See, for example, [Humphreys, 1976], [Humphreys and Verma, 1973] and [Ballard, 1978].

Let V be a projective, indecomposable G_1-module. Then there exists a G-module which restricts to V as a G_1-module.

The first person to study this conjecture in detail was Ballard in [Ballard, 1978]. He was able to prove this conjecture for $p \geqslant 3h-3$, where h is the Coxeter number of G. This bound was then improved in [Jantzen, 1980][10] to $p \geqslant 2h-2$. For arbitrary primes, however, the question remains open. Up until 2019, it was believed that a solution to this problem would come through Donkin's Tilting Module Conjecture, which in essence conjectured that all projective indecomposable G_r-modules could be extended to indecomposable tilting G-modules. Instead, the recent paper [Bendel et al., 2019] is able to provide a counterexample to the Tilting Module Conjecture. Thus, the search for new methods to address the Humphreys-Verma conjecture continues.

In this thesis, two such methods are given. These methods were developed jointly with Dmitriy Rumynin, and also appear in [Rumynin and Westaway, 2018] and [Rumynin and Westaway, 2019].

The first of which, in Chapter 5, is best understood through the lens of abstract groups. In particular, the question at issue is whether (projective, indecomposable) G_1-modules can be extended to G-modules, so as an initial matter we can examine when a representation (V,θ) of a normal subgroup N of an abstract group H can be extended to a representation of H.[11] If a representation Θ of H indeed restricts to θ, we must have that (V,θ) is equivalent to the twisted representation (V,θ^h) for all $h \in H$. In fact, the intertwiner of the two representations can be chosen to be $\Theta(h)$. So one may naturally ask the question: if a representation (V,θ) of N satisfies $(V,\theta) \cong (V,\theta^h)$ for all $h \in H$ can we choose intertwiners $T_h \in \mathrm{GL}(V)$ such that the map $\Theta : H \to \mathrm{GL}(V)$ sending h to T_h is a representation of H extending θ?

It turns out that this reduces to asking whether the intertwiners can be chosen such that $h \mapsto T_h$ is a homomorphism. Furthermore, it can be shown that, for $h_1, h_2 \in H$, the intertwiners can be chosen such that the linear map $T_{h_1}T_{h_2}T_{h_1h_2}^{-1}$ is an N-module automorphism of V. If the group of N-module automorphisms of V is soluble, with suitable subnormal series $\mathrm{Aut}_N(V) \rhd A_1 \rhd \ldots \rhd A_k = \{1\}$, we then give in Theorem 5.1.2.4 a process to determine whether, in fact, one can chose the intertwiners such that the $T_{h_1}T_{h_2}T_{h_1h_2}^{-1}$ instead all lie in A_1. This depends on the vanishing of a certain cocycle in a suitable second cohomology group. Iterating the process, we conclude that the vanishing of certain cocycles is enough to show that the $T_{h_1}T_{h_2}T_{h_1h_2}^{-1}$ lie in $A_k = \{1\}$, which gives the algorithm in Theorem 5.1.3.1, and more specific existence and uniqueness tests in Corollary 5.1.3.2 and Corollary 5.1.3.3.

Adapting this method to algebraic groups and group schemes requires the fixing

[10] See also II.11.11 in [Jantzen, 1987].

[11] This question has also been looked at in [Dade, 1981] and [Thévenaz, 1983], and our approach bears some similarities with theirs. In particular, Theorem 5.1.3.1 generalises Corollary 1.8 and Proposition 2.1 in [Thévenaz, 1983] to the case of a soluble automorphism group $\mathrm{Aut}_L(V)$. We also use different cohomology groups than Dade and Thévenaz, in order to be able to translate our approach to algebraic groups.

of some technicalities, which we do in Section 5.2, but the result ends up holding in this case as well in Theorem 5.2.4.1. This leads to some cohomological conditions for the existence (and uniqueness) of such an extension.

The second approach, in Chapter 6, makes use of exponentials. As discussed above, when looking at Lie groups or algebraic groups over $\mathbb{C}$, the general method to integrate finite-dimensional representations is to use exponentials. In positive characteristic, however, problems quickly arise in trying to use this method.

Specifically, given a restricted representation (V, θ) of $\mathfrak{g}$, we can define for each $x \in N_p(\mathfrak{g})$ (the p-nilpotent cone of $\mathfrak{g}$) the exponential

$$e^{\theta(x)} = \sum_{k=0}^{p-1} \frac{1}{k!}\theta(x)^k \in \mathfrak{gl}(V)$$

and the algebraic group $G_V \leqslant \mathrm{GL}(V)$ generated by these exponentials. We would like these elements to satisfy the equation $\theta(e^{ad(x)}(y)) = e^{\theta(x)}\theta(y)e^{-\theta(x)}$ for all $x \in N_p(\mathfrak{g})$, $y \in \mathfrak{g}$. However, this will only hold in general if θ is *over-restricted*, that is, if $\theta(x)^{\lfloor (p+1)/2 \rfloor} = 0$ for all $x \in N_p(\mathfrak{g})$.

If the representation is, in fact, over-restricted, then we prove in Corollary 6.1.1.7 and Corollary 6.1.1.8 that under certain restrictions (including on the size of p) θ can be lifted to a representation of G_V, which leads to a representation of G. It is conjectured (Higher Frobenius Conjecture) that a similar process could be applied for higher Frobenius kernels; if this holds then we find in Proposition 6.2.1.2 that, under certain conditions, to integrate a projective indecomposable module from G_1 to G it is enough to integrate from G_1 to some higher Frobenius kernel G_r.

Layout

After this introduction, the thesis starts with *Chapter 2: Preliminaries.* Here, the background definitions and results necessary to understand the rest of the thesis are explained, largely without proofs. This includes a discussion of Lie algebras in positive characteristic in Section 2.1, Hopf algebras and Hopf-Galois extensions in Section 2.2, algebraic groups in positive characteristic in Section 2.3, and the representation theory of reductive Lie algebras and algebraic groups in Section 2.4.

Chapter 3: Higher Deformations - Constructions then begins the study of Friedlander and Parshall's question. After a brief detour about the connection to the theory of differential operators in Section 3.1, the initial construction of the higher universal enveloping algebras $U^{[r]}(G)$ is given in Section 3.2. This section also shows how these algebras are connected to the universal enveloping algebras $U(\mathfrak{g})$. Sections 3.3 and 3.4 then prove a number of structural results about these algebras, including the existence of a p-centre and a Poincaré-Birkhoff-Witt basis. The construction of the higher reduced enveloping algebras $U_\chi^{[r]}(G)$, as desired by Friedlander and Parshall, is then conducted in Section 3.5, where some basic properties of these algebras are also given.

The next chapter, *Chapter 4: Higher Deformations - Representation Theory*, delves into the representation theory of the higher reduced universal enveloping algebras $U_\chi^{[r]}(G)$ when G is reductive. Specifically, focusing on irreducible representations, in Section 4.1 an analogue for Steinberg's tensor product theorem is proved for the $U_\chi^{[r]}(G)$, the teenage Verma modules $Z_\chi^r(P,\lambda)$ are constructed, and a number of consequences are derived. Then, Section 4.2 explores some questions related to the centres and Azumaya loci of the $U^{[r]}(G)$.

Chapter 5: Integration of Modules - Stability then turns to the Humphreys-Verma conjecture and related topics, and tackles the first approach to the problem. This begins with Section 5.1, which deals with the case of abstract groups. Specifically, it introduces (L,H)-morphs and gives the construction of an "exact sequence" which is then used to give an algorithm giving cohomological conditions on whether modules can be extended from normal subgroups. Section 5.2 then repeats this process for algebraic groups, naturally having to spend more time on some of the algebro-geometric problems that arise in this case.

The thesis concludes with the second approach to Humphreys-Verma related problems in *Chapter 6: Integration of Modules - Exponentials.* Section 6.1 defines over-restricted and r-over-restricted representations of $\mathfrak{g}$, and proves (or conjectures) some results concerning when these representations can be integrated to representations of G. Applications of these results to the Humphreys-Verma conjecture itself are then given in Section 6.2.

Chapter 2

Preliminaries

2.1 Lie algebras in positive characteristic

2.1.1 Lie algebras and universal enveloping algebras

A **Lie algebra** over an algebraically closed field[12] $\mathbb{K}$ is a $\mathbb{K}$-vector space $\mathfrak{g}$ equipped with a bilinear map $[\cdot,\cdot] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ (the **Lie bracket** of $\mathfrak{g}$) which satisfies

1. $[x, x] = 0$ for all $x \in \mathfrak{g}$.
2. $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ for all $x, y, z \in \mathfrak{g}$.

The Lie bracket of $\mathfrak{g}$ clearly satisfies $[x, y] = -[y, x]$ for all $x, y \in \mathfrak{g}$, and we call $\mathfrak{g}$ **abelian** if $[x, y] = 0$ for all $x, y \in \mathfrak{g}$. A **homomorphism of Lie algebras** $f : (\mathfrak{g}_1, [\cdot,\cdot]_1) \to (\mathfrak{g}_2, [\cdot,\cdot]_2)$ is a linear map $f : \mathfrak{g}_1 \to \mathfrak{g}_2$ such that $f([x, y]_1) = [f(x), f(y)]_2$ for all $x, y \in \mathfrak{g}_1$.

One common source of Lie algebras is associative algebras: an associative algebra A can be made into a Lie algebra by defining the Lie bracket $[x, y] = xy - yx$ for all $x, y \in A$. This Lie algebra is denoted $A^{(-)}$. For example, this process allows us to define the Lie algebra $\mathfrak{gl}_n := M_n(\mathbb{K})^{(-)}$ and its Lie subalgebra

$$\mathfrak{sl}_n := \{A \in M_n(\mathbb{K})^{(-)} \mid \mathrm{Trace}(A) = 0\}.$$

The **universal enveloping algebra** of a Lie algebra $\mathfrak{g}$ is the associative algebra

$$U(\mathfrak{g}) := \frac{T(\mathfrak{g})}{Q}$$

where $T(\mathfrak{g})$ is the tensor algebra of $\mathfrak{g}$ and Q is the 2-sided ideal generated by the elements

$$x \otimes y - y \otimes x - [x, y]$$

[12] In this thesis we only consider algebraically closed fields. Some statements, especially in this chapter, will hold in greater generality; however, the benefits to taking a case-by-case approach are outweighed by a desire for clarity and consistency.

for $x, y \in \mathfrak{g}$. Letting $\iota : \mathfrak{g} \to U(\mathfrak{g})^{(-)}$ be the natural Lie algebra homomorphism, the following proposition justifies the "universal" nomenclature.

Proposition 2.1.1.1. *Let A be an associative algebra, and let $\theta : \mathfrak{g} \to A^{(-)}$ be a Lie algebra homomorphism. Then there exists a unique homomorphism of associative algebras $\widetilde{\theta} : U(\mathfrak{g}) \to A$ such that $\widetilde{\theta}\iota = \theta$.*

A priori, it is not clear that ι need be an injective map. However, this fact follows from the following explicit description of a basis of $U(\mathfrak{g})$. We state the theorem for finite-dimensional $\mathfrak{g}$, although it can be generalised to the infinite-dimensional case.

Theorem 2.1.1.2 (Poincaré-Birkhoff-Witt Theorem)**.** *If $x_1, \ldots, x_n$ is a basis of $\mathfrak{g}$, then $U(\mathfrak{g})$ has a basis consisting of the elements*[13] $x_1^{a_1} \ldots x_n^{a_n}$ *with $a_i \geqslant 0$ for all i.*

2.1.2 Representations of Lie algebras

One of the key reasons for defining universal enveloping algebras is their connection with representation theory. A **$\mathfrak{g}$-module** (equivalently, a **representation**[14] of $\mathfrak{g}$) is defined to be a pair (V, θ) where V is a $\mathbb{K}$-vector space and θ is Lie algebra homomorphism $\mathfrak{g} \to \mathfrak{gl}(V)$. Given $x \in \mathfrak{g}$ and $v \in V$ we often write $x \cdot v$, or simply xv, for the element $\theta(x)(v)$. The universal property of $U(\mathfrak{g})$ implies that there is an equivalence of categories between $\mathfrak{g}$-modules and $U(\mathfrak{g})$-modules.

We are particularly interested in *irreducible* and *indecomposable* $\mathfrak{g}$-modules.

Definition. *Let (V, θ) be a $\mathfrak{g}$-module.*

(1) *We call a subspace W of V* **$\mathfrak{g}$-invariant** *if $\theta(x)(w) \in W$ for all $x \in \mathfrak{g}$ and $w \in W$.*

(2) *We say that (V, θ) is* **irreducible** *if $V \neq 0$ and the only $\mathfrak{g}$-invariant subspaces of V are 0 and V.*

(3) *We say that (V, θ) is* **indecomposable** *if the only pairs of $\mathfrak{g}$-invariant subspaces X and W such that $V = X \oplus W$ are $(X, W) = (0, V)$ and $(X, W) = (V, 0)$.*

Remark 1. *All irreducible $\mathfrak{g}$-modules are clearly indecomposable. Over a field of characteristic zero, it is also true that all finite-dimensional indecomposable modules are irreducible. However, this converse can fail in positive characteristic. See, for example, [Jacobson, 1952] (exhibiting a $\mathfrak{g}$-module which can be decomposed into a direct sum of indecomposable modules, but not a direct sum of irreducible ones).*

To obtain some examples of Lie algebra representations, let G be an affine algebraic group[15] and let $\mathbb{K}[G]$ be its coordinate algebra (i.e. the algebra of regular

[13] Note that in the universal enveloping algebra $U(\mathfrak{g})$ we generally suppress the tensor product notation and simply write xy for $x \otimes y$.

[14] Throughout this thesis we avoid parsing the difference between modules and representations and the words will be used interchangeably.

[15] See Subsection 2.3.1, *infra*, for further discussion of affine algebraic groups.

functions $G \to \mathbb{K}$). A morphism $G \to G$ gives rise to a ring endomorphism of $\mathbb{K}[G]$, and in this manner we can construct, for each $x \in G$, an endomorphism λ_x of $\mathbb{K}[G]$ corresponding in G to left multiplication by x.

We further recall that a linear map $D : \mathbb{K}[G] \to \mathbb{K}[G]$ is called a **derivation** if

$$D(fg) = fD(g) + D(f)g$$

for all $f, g \in \mathbb{K}[G]$, and we denote by $\mathrm{Der}_{\mathbb{K}}(\mathbb{K}[G])$ the vector space of all such derivations. This is in fact a Lie algebra under the Lie bracket $[D_1, D_2] := D_1 \circ D_2 - D_2 \circ D_1$.

The Lie algebra of G, which we write as $\mathrm{Lie}(G)$ or as $\mathfrak{g}$, is then defined to be

$$\mathrm{Lie}(G) := \{D \in \mathrm{Der}_{\mathbb{K}}(\mathbb{K}[G]) \mid \lambda_x \circ D = D \circ \lambda_x \text{ for all } x \in G\},$$

which one can check is a (finite-dimensional) Lie subalgebra of $\mathrm{Der}_{\mathbb{K}}(\mathbb{K}[G])$.

2.1.3 Structure in positive characteristic

Given two derivations τ and σ in $\mathrm{Lie}(G) = \mathfrak{g}$, it is not true in general that $\sigma \circ \tau$ is a derivation. However, when the field $\mathbb{K}$ has characteristic $p > 0$, we have the following equation:

$$\tau^p(fg) = \sum_{i=0}^{p} \binom{p}{i} \tau^i(f)\tau^{p-i}(g) = f\tau^p(g) + \tau^p(f)g.$$

In other words, τ^p is a derivation and furthermore it is left invariant. Hence, we define a map ${}^{[p]} : \mathfrak{g} \to \mathfrak{g}$ which sends $\delta \in \mathfrak{g}$ to $\delta^{[p]} := \delta^p$.[16] For the rest of this section we assume that the characteristic of $\mathbb{K}$ is $p > 0$.

Proposition 2.1.3.1. *The map* ${}^{[p]} : \mathfrak{g} \to \mathfrak{g}$ *satisfies the following two properties:*

(1) *The map* $\xi : \mathfrak{g} \to U(\mathfrak{g})$ *given by sending* $x \in \mathfrak{g}$ *to* $x^p - x^{[p]}$ *in* $U(\mathfrak{g})$ *has image in the centre of* $U(\mathfrak{g})$.

(2) *The map* ξ *is semilinear, i.e.* $\xi(ax + by) = a^p\xi(x) + b^p\xi(y)$ *for all* $a, b \in \mathbb{K}$, $x, y \in \mathfrak{g}$.

Proof. See A.2 in [Jantzen, 2004]. □

Definition. *A (finite-dimensional) Lie algebra* $\mathfrak{g}$ *equipped with a map* ${}^{[p]} : \mathfrak{g} \to \mathfrak{g}$ *which satisfies the conclusions of Proposition 2.1.3.1 is called a* **restricted Lie algebra**, *and* ${}^{[p]}$ *is called the p-th power map on* $\mathfrak{g}$.

[16] From this point on, for $\delta \in \mathfrak{g}$, we always write $\delta^{[p]}$ for the p-times composition of δ with itself, and use δ^p to mean the p-th power of δ as an element of the associative algebra $U(\mathfrak{g})$.

Remark 2. *We may, of course, define restricted Lie algebras of arbitrary dimension using the same criteria. However, many of the results that follow require finite-dimensionality of $\mathfrak{g}$ in order to hold, so for this thesis we limit ourselves to the study of restricted Lie algebras of finite dimension.*

Given a homomorphism of algebraic groups $f : G_1 \to G_2$, we obtain the **derivative** $df : \mathrm{Lie}(G_1) \to \mathrm{Lie}(G_2)$ as the derivative of the underlying morphism of varieties (we call this process **differentiation**). The map df is a Lie algebra homomorphism. Since $\mathrm{Lie}(\mathrm{GL}(V)) = \mathfrak{gl}(V)$ for a $\mathbb{K}$-vector space V, if $\Theta : G \to GL(V)$ is a homomorphism of algebraic groups, i.e. a representation of G, then differentiating gives $d\Theta : \mathfrak{g} \to \mathfrak{gl}(V)$. This hence equips V with the structure of a $\mathfrak{g}$-module.

Proposition 2.1.3.2. *The representation $d\Theta$ of $\mathfrak{g}$ satisfies the equation $d\Theta(x^{[p]}) = d\Theta(x)^p$ for all $x \in \mathfrak{g}$.*

Proof. See Section I.3.19 in [Borel, 1991]. □

As discussed in the introduction, over a field of characteristic zero all representations of a Lie algebra $\mathrm{Lie}(G)$ are derivatives of representations of the algebraic group G, if G is semisimple and simply-connected. Proposition 2.1.3.2 is the key reason why this fails in positive characteristic.

Definition. *Let $\mathfrak{g}$ be a restricted Lie algebra. A $\mathfrak{g}$-module (V, θ) is called* **restricted** *if $\theta(x)^p = \theta(x^{[p]})$ for all $x \in \mathfrak{g}$.*

Even without limiting ourselves to restricted representations, the existence of a p-th power map on $\mathfrak{g}$ has some significant consequences for its representation theory, as the following results show.

Proposition 2.1.3.3. *If $\mathfrak{g}$ is a restricted Lie algebra then all irreducible $\mathfrak{g}$-modules are finite-dimensional. Furthermore, the dimension of these irreducible modules is bounded by $p^{\dim(\mathfrak{g})}$.*

Proof. See A.4 in [Jantzen, 2004]. □

Proposition 2.1.3.4. *If $\mathfrak{g}$ is a restricted Lie algebra and V is an irreducible $\mathfrak{g}$-module (hence an irreducible $U(\mathfrak{g})$-module) then there exists $\chi \in \mathfrak{g}^*$ such that, for any $v \in V$ and $x \in \mathfrak{g}$,*

$$(x^p - x^{[p]}) \cdot v = \chi(x)^p v.$$

We call χ the **p-character** *of V.*

Proof. Since $x^p - x^{[p]}$ is central in $U(\mathfrak{g})$ the linear map $f : V \to V$ which sends $v \in V$ to $(x^p - x^{[p]}) \cdot v$ is a $U(\mathfrak{g})$-module endomorphism. Since V is finite-dimensional, the result then follows from Schur's lemma[17] and the semilinearity of the map $x \mapsto x^p - x^{[p]}$. □

[17]**Schur's lemma:** Let A be an algebra over an algebraically closed field $\mathbb{K}$, and let V be a finite-dimensional irreducible A-module. Then $\mathrm{End}_A(V)$ is a division ring. Furthermore, if $f : V \to V$ is an A-linear endomorphism then there exists $\lambda \in \mathbb{K}$ such that $f(v) = \lambda v$ for all $v \in V$.

This proposition motivates the following definition. For $\chi \in \mathfrak{g}^*$, define

$$U_\chi(\mathfrak{g}) := \frac{U(\mathfrak{g})}{\langle x^p - x^{[p]} - \chi(x)^p \mid x \in \mathfrak{g} \rangle}.$$

We call $U_\chi(\mathfrak{g})$ a **reduced enveloping algebra** of $\mathfrak{g}$, and we call $U_0(\mathfrak{g})$ the **restricted enveloping algebra** of $\mathfrak{g}$.

Corollary 2.1.3.5. *Every irreducible $\mathfrak{g}$-module is an irreducible $U_\chi(\mathfrak{g})$-module for some $\chi \in \mathfrak{g}^*$.*

Remark 3. *This corollary can be used to improve the upper bound on the dimension of irreducible $\mathfrak{g}$-modules to $p^{\dim(\mathfrak{g})/2}$, as in Section 2.8 of [Jantzen, 1997].*

Observe that restricted representations of $\mathfrak{g}$ are precisely those which factor through $U_0(\mathfrak{g})$. In particular, this implies that $\mathfrak{g}$-modules which factor through $U_\chi(\mathfrak{g})$ for $\chi \neq 0$ are not derived from G-modules. The following proposition gives a analogue of the Poincaré-Birkhoff-Witt Theorem for reduced enveloping algebras.[18]

Proposition 2.1.3.6. *For $\chi \in \mathfrak{g}^*$, the reduced enveloping algebra $U_\chi(\mathfrak{g})$ is an associative $\mathbb{K}$-algebra of dimension $p^{\dim(\mathfrak{g})}$. Furthermore, if $x_1, \ldots, x_n$ is a basis of $\mathfrak{g}$, then $U_\chi(\mathfrak{g})$ has basis*

$$\{x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n} \mid 0 \leqslant a_i < p \text{ for all } 1 \leqslant i \leqslant n\}.$$

For each $g \in G$, we can define a homomorphism $c_g : G \to G$ which sends h to ghg^{-1}. Differentiating gives a Lie algebra homomorphism $Ad(g) := dc_g : \mathfrak{g} \to \mathfrak{g}$, and hence an action of G on $\mathfrak{g}$ called the **adjoint action**. We can furthermore use this to define an action of G on $\mathfrak{g}^*$, called the **coadjoint action**. This is defined by $g \cdot \chi(x) = \chi(Ad(g)^{-1}(x))$ for $g \in G$, $\chi \in \mathfrak{g}^*$ and $x \in \mathfrak{g}$.

Proposition 2.1.3.7. *For each $g \in G$, there is an isomorphism*

$$U_\chi(\mathfrak{g}) \cong U_{g \cdot \chi}(\mathfrak{g}).$$

Proof. See A.8 in [Jantzen, 2004]. □

2.2 Hopf algebras

2.2.1 Definitions

In Subsection 2.1.1, *supra*, we reviewed the construction and properties of the universal enveloping algebra of a Lie algebra $\mathfrak{g}$. In Subsection 2.3.2, *infra*, we discuss the distribution algebra $\mathrm{Dist}(G)$ of an algebraic group G. An important commonality between the algebras $U(\mathfrak{g})$ and $\mathrm{Dist}(G)$ is that they are both *Hopf algebras.*

[18] See A.7 in [Jantzen, 2004].

To proceed with their study we therefore need to discuss some properties of Hopf algebras. In this section, we take $\mathbb{K}$ to be an algebraically closed field of arbitrary characteristic.

Recall that a $\mathbb{K}$-**algebra**[19] is a triple (A, m, u), where A is a $\mathbb{K}$-vector space and $m : A \otimes A \to A$ (multiplication) and $u : \mathbb{K} \to A$ (unit) are linear maps,[20] with the property that

$$m \circ (m \otimes id) = m \circ (id \otimes m), \quad \text{and} \quad m \circ (u \otimes id) = id = m \circ (id \otimes u).$$

We say that A is **commutative** if $m(a \otimes b) = m(b \otimes a)$ for all $a, b \in A$. Furthermore, a **homomorphism** of $\mathbb{K}$-algebras $f : (A, m, u) \to (A', m', u')$ is a linear map $f : A \to A'$ such that

$$m' \circ (f \otimes f) = f \circ m, \quad \text{and} \quad f \circ u = u'.$$

By dualising, we obtain the definitions for coalgebras. Namely, a $\mathbb{K}$-coalgebra is a triple (C, Δ, ε), where C is a $\mathbb{K}$-vector space and $\Delta : C \to C \otimes C$ (comultiplication) and $\varepsilon : \mathbb{K} \to A$ (counit) are linear maps, with the property that

$$(\Delta \otimes id) \circ \Delta = (id \otimes \Delta), \quad \text{and} \quad (\varepsilon \otimes id) \circ \Delta = id = (id \otimes u) \circ \Delta.$$

Note that we use Sweedler's Σ-notation for comultiplication, i.e., for $c \in C$ we write

$$\Delta(c) = \sum c_{(1)} \otimes c_{(2)} \in C \otimes C.$$

A coalgebra is called **cocommutative** if $\sum c_{(1)} \otimes c_{(2)} = \sum c_{(2)} \otimes c_{(1)}$ for all $c \in C$. A **homomorphism** of $\mathbb{K}$-coalgebras $f : (C, \Delta, \varepsilon) \to (C', \Delta', \epsilon')$ is a linear map $f : C \to C'$ such that

$$(f \otimes f) \circ \Delta = \Delta' \circ f, \quad \text{and} \quad \varepsilon' \circ f = \varepsilon.$$

Suppose that (A, m, u) is a $\mathbb{K}$-algebra and (C, Δ, ε) is a $\mathbb{K}$-coalgebra. Then the vector space $\mathrm{Hom}_{\mathbb{K}}(C, A)$ can be made into an algebra whose multiplication, called the **convolution product**, is described via

$$(f * g)(c) = \sum f(c_{(1)}) g(c_{(2)})$$

for $f, g \in \mathrm{Hom}_{\mathbb{K}}(C, A)$ and $c \in C$. The unit of this algebra is $u\varepsilon$, and we say that $f \in \mathrm{Hom}_{\mathbb{K}}(C, A)$ is **convolution invertible** if there exists $g \in \mathrm{Hom}_{\mathbb{K}}(C, A)$ such that $f * g = u\varepsilon = g * f$.

[19]We may simply refer to $\mathbb{K}$-algebras as **algebras** when the field is clear. Furthermore, the reader should note that in this section when we discuss algebras without any further qualifier we are referring to associative algebras.

[20]Here, and throughout this thesis, an unadorned tensor product $\otimes$ shall be taken to mean tensor product over the ground field $\mathbb{K}$, i.e. $\otimes_{\mathbb{K}}$.

We may also discuss modules (resp. comodules) over algebras (resp. coalgebras). If (A, m, u) is an algebra (resp. (C, Δ, ε) a coalgebra) then a **left A-module** (resp. **left C-comodule**) is a $\mathbb{K}$-vector space M equipped with a linear map $\rho : A \otimes M \to M$ (resp. $\omega : M \to C \otimes M$) such that

$$\rho \circ (m \otimes id) = \rho \circ (id \otimes m), \quad \text{and} \quad \rho \circ (u \otimes id) = id$$

$$(\text{resp. } (\Delta \otimes id) \circ \omega = (id \otimes \Delta) \circ \omega, \quad \text{and} \quad (\varepsilon \otimes id) \circ \omega = id).$$

(Note that we also use Sweedler's Σ-notation for comodules. In particular, if M is a C-module, we write $\omega(m) = \sum m_{(1)} \otimes m_{(2)}$ for $m \in M$, where $m_{(1)} \in C$ and $m_{(2)} \in M$.) We can similarly define right modules[21] (resp. right comodules). A **homomorphism of left A-modules** (resp. **C-comodules**) is then a linear map $f : M \to M'$ such that

$$f \circ \rho = \rho \circ (id \otimes f) \quad (\text{resp. } \omega' \circ f = (id \otimes f) \circ \omega).$$

Notation. *We denote by* $\mathrm{Mod}(A)$ *the category of all (left) A-modules,* $\mathrm{mod}(A)$ *the category of all finite-dimensional (left) A-modules, and* $\mathrm{Irr}(A)$ *the category of all irreducible (left) A-modules.*[22]

We may combine the structure of an algebra and a coalgebra to obtain a bialgebra. Namely, a **$\mathbb{K}$-bialgebra**[23] is a vector space B equipped with maps m, u, Δ and ε such that (B, m, u) is an algebra, (B, Δ, ε) is a coalgebra, and the maps $\Delta : B \to B \otimes B$ and $\varepsilon : B \to \mathbb{K}$ are algebra homomorphisms.[24] Equivalent to the latter condition is the requirement that the maps $m : B \otimes B \to B$ and $u : \mathbb{K} \to B$ are *coalgebra* homomorphisms.[25] If $(B, m, u, \Delta, \varepsilon)$ and $(B', m', u', \Delta', \varepsilon')$ are bialgebras, a **bialgebra homomorphism** is a linear map $f : B \to B'$ which is both an algebra homomorphism and a coalgebra homomorphism.

We can now give the definition of a Hopf algebra.

Definition. *A* **$\mathbb{K}$-Hopf algebra**[26] *is a $\mathbb{K}$-bialgebra $(H, m, u, \Delta, \varepsilon)$ equipped with a $\mathbb{K}$-linear map $S : H \to H$, which we call the* **antipode** *of H, such that the diagram*

---

[21] In this thesis, the word *module* without qualifier will be taken to mean a left module.

[22] Recall that a module M over an algebra A is called irreducible if has no proper non-zero submodules. We do not distinguish notationally between the category of irreducible modules and the category of finite-dimensional irreducible modules, since for almost all A relevant to this thesis they will be identical.

[23] If the field $\mathbb{K}$ is clear, we may simply refer to a bialgebra instead of a $\mathbb{K}$-bialgebra.

[24] Note here that $B \otimes B$ is a $\mathbb{K}$-algebra with multiplication induced by $m_{B \otimes B}(b_1 \otimes b_2, b_1' \otimes b_2') = b_1 b_1' \otimes b_2 b_2'$, for $b_1, b_1', b_2, b_2' \in B$, and with unit $1 \otimes 1$.

[25] Here, $B \otimes B$ is a coalgebra with comultiplication induced by $\Delta_{B \otimes B}(b \otimes b') = \sum (b_1 \otimes b_1') \otimes (b_2 \otimes b_2')$ and with counit sending $b \otimes b'$ to $\varepsilon(b)\varepsilon(b')$.

[26] If the field $\mathbb{K}$ is clear, we may simply refer to a Hopf algebra instead of a $\mathbb{K}$-Hopf algebra.

$$\begin{tikzcd}
H & H \otimes H \arrow[l, "S\otimes id"'] \arrow[r, "id\otimes S"] & H \\
\mathbb{K} \arrow[u, "u"] & H \arrow[l, "\varepsilon"'] \arrow[r, "\varepsilon"] \arrow[u, "\Delta"] & \mathbb{K} \arrow[u, "u"]
\end{tikzcd}$$

commutes.

The reader should note that the condition on S precisely means that S is convolution invertible in $\mathrm{Hom}_{\mathbb{K}}(H, H)$.

Definition. *Let $(H, m, u, \Delta, \varepsilon, S)$ and $(H', m', u', \Delta', \varepsilon', S')$ be Hopf algebras. A* **Hopf algebra homomorphism** *$f : (H, m, u, \Delta, \varepsilon, S) \to (H', m', u', \Delta', \varepsilon', S')$ is a bialgebra homomorphism such that $S'f(h) = fS(h)$ for all $h \in H$.*

Definition. *Let $(H, m, u, \Delta, \varepsilon, S)$ be a Hopf algebra.*[27] *Let A be a vector subspace of H.*

(1) *We say that A is a* **Hopf subalgebra** *of H if A is a subalgebra*[28] *of H, $\Delta(A) \subseteq A \otimes A$ and $S(A) \subseteq A$.*

(2) *We say that A is a* **Hopf ideal** *of H if A is a (two-sided) ideal*[29] *of H, $\Delta(A) \subseteq A \otimes H + H \otimes A$, $S(A) \subseteq A$ and $\varepsilon(A) = 0$.*

Remark 4. *If I is a Hopf ideal of H then the quotient algebra H/I can be equipped with the structure of a Hopf algebra, where*

$$\Delta(h + I) = \sum (h_{(1)} + I) \otimes (h_{(2)} + I),$$

$$\varepsilon(h + I) = \varepsilon(h)$$

and

$$S(h + I) = S(h) + I.$$

Furthermore, the natural surjection $H \to H/I$ is a homomorphism of Hopf algebras.

Since a Hopf algebra H is both an algebra and a coalgebra, we can speak of both H-modules and H-comodules. The additional structure of a Hopf algebra enables us to construct tensor products of modules and comodules. Namely, if M and N are left H-modules, then $M \otimes N$ can be equipped with the structure of a left H-module via the action

$$h \cdot (m \otimes n) = \sum (h_{(1)}m) \otimes (h_{(2)}n).$$

[27] From now on, we may avoid the full notation by simply referring to the Hopf algebra H. In this case, we implicitly denote the maps by $m, u, \Delta, \varepsilon$ and S, or, if there may be ambiguity, $m_H, u_H, \Delta_H, \varepsilon_H$ and S_H.

[28] Recall that a **subalgebra** A of a $\mathbb{K}$-algebra H is a $\mathbb{K}$-vector subspace of H such that $m_H(A \otimes A) \subseteq A$ and $u_H(\mathbb{K}) \subseteq A$

[29] Recall that a **(two-sided) ideal** I of a $\mathbb{K}$-algebra H is a $\mathbb{K}$-vector subspace of H such that $m_H(H \otimes I + I \otimes H) \subseteq I$.

Similarly, if M and N are left comodules, then we can equip $M \otimes N$ with the comodule structure

$$m \otimes n \mapsto \sum m_{(1)} n_{(1)} \otimes m_{(2)} \otimes n_{(2)}.$$

We can, of course, similarly define tensor products of right modules and comodules.

Definition. *Let H be a Hopf algebra and A an algebra. We say that A is a* **(right) H-comodule algebra** *if (A, ω) is a right H-comodule and the multiplication and unit maps of A are H-comodule morphisms.*[30] *We denote*

$$A^{coH} := \{a \in A \mid \omega(a) = a \otimes 1\}$$

and call elements of A^{coH} **H-coinvariants** *of A*

Remark 5. *If H is a Hopf algebra and $I \subseteq H$ is a Hopf ideal, then H can be made into an H/I-comodule algebra, via the H/I-comodule map*

$$h \mapsto \sum h_{(1)} \otimes (h_{(2)} + I).$$

2.2.2 Extensions

When studying the representation theory of abstract groups a powerful tool is the ability to induce representations from subgroups. When the subgroups in question are normal, there are a number of significant results about how this induction process behaves; the study of this situation is called *Clifford theory.* Later on in this thesis we shall want to exploit Clifford theory type results for Hopf algebras. Before we can do that, however, we need to talk about extensions of Hopf algebras.

Definition. *Let A be a Hopf algebra. Given $a, b \in A$, we define*

$$ad_l(a)(b) = \sum a_{(1)} b S(a_{(2)})$$

and

$$ad_r(a)(b) = \sum S(a_{(1)}) b a_{(2)}.$$

The maps ad_l and ad_r are called the **left** *and* **right adjoint actions***, respectively, of A on itself.*

Definition. *Let A be a Hopf algebra and $B \subseteq A$ a Hopf subalgebra of A. We say that B is* **normal** *in A if $ad_l(a)(b) \in B$ and $ad_r(a)(b) \in B$ for all $a \in A$ and $b \in B$.*

Note that if A is cocommutative it is sufficient to check this property for either the left adjoint or the right adjoint action. For the following result, note that given a Hopf algebra H with counit ε we define

$$H^+ := H \cap \ker \varepsilon.$$

[30] The comodule structure on $A \otimes A$ is as described above. The comodule structure on $\mathbb{K}$ comes from $1_{\mathbb{K}} \mapsto 1_{\mathbb{K}} \otimes 1_H$.

Proposition 2.2.2.1. *Let A be a Hopf algebra and B a normal Hopf subalgebra of A. Then $AB^+ = B^+A$ and this is a Hopf ideal of A.*

Proof. See Lemma 3.4.2(1) in [Montgomery, 1993]. ☐

In particular, in this situation we have an injective Hopf algebra homomorphism $B \hookrightarrow A$ and a surjective Hopf algebra homomorphism $A \twoheadrightarrow A/AB^+$.

Definition. *Let H be a Hopf algebra, (A, ω) a right H-comodule algebra, and B a subalgebra of A with $A^{coH} = B$. We then call $B \subseteq A$ a* **(right) H-extension**.

Definition. *Let $B \subseteq A$ be a right H-extension. We say that $B \subseteq A$ is a* **(right) H Galois-extension**[31] *if the natural linear map*

$$A \otimes_B A \to A \otimes_{\mathbb{K}} H, \qquad a \otimes_B a' \mapsto (a \otimes 1)\omega(a')$$

is bijective.

The following proposition indicates that we have already seen one source of Hopf-Galois extensions.

Proposition 2.2.2.2. *Let A be a Hopf algebra and B a normal Hopf subalgebra of A. Set $H := A/AB^+$. If A is cocommutative then $B \subseteq A$ is an H-Galois extension.*

Proof. See Remark 1.1(4) in [Schneider, 1990]. ☐

In order to obtain Clifford theory type results for Hopf algebras, we need to understand the ways in which a normal Hopf subalgebra can lie inside a Hopf algebra. The next few definitions and propositions give some perspectives on this.

Definition. *Let A be a Hopf algebra and B a normal Hopf subalgebra of A.*

(1) *We say that A is* **free** *over B if A is free as a left B-module under left multiplication.*

(2) *We say that A is* **faithfully flat** *over B if, whenever $f : N \to M$ is a homomorphism of left B-modules, f is injective if and only if the corresponding A-module homomorphism $id_A \otimes f : A \otimes_B N \to A \otimes_B M$ is injective.*

Proposition 2.2.2.3. *Let A be a Hopf algebra and B a normal Hopf subalgebra of A. The following results hold.*

(1) *If A is free over B then it is faithfully flat over B.*

(2) *If B is finite-dimensional over $\mathbb{K}$, then A is free over B.*

Proof. It is straightforward to prove (1) from the definitions. Theorem 2.1(2) in [Schneider, 1993] proves (2). ☐

[31] We may call this a Hopf-Galois extension if we do not wish to specify H.

In order to understand Hopf-Galois extensions, we need a way to construct a comodule algebra from an algebra and a Hopf algebra. This mirrors the way in which we study extensions of abstract groups. To define these comodule algebras, we first need to make some further definitions.

Definition. *Let H be a Hopf algebra and B an algebra. Let $\sigma : H \otimes H \to B$ be a convolution invertible linear map.*

(1) *H is said to* **measure** *B if there exists a linear map $H \otimes B \to B$, which we write as $h \otimes b \mapsto h \cdot b$, such the following two conditions hold:*

   (a) $h \cdot 1 = \varepsilon(h)1$ for all $h \in H$.

   (b) $h \cdot (ab) = \sum (h_{(1)} \cdot a)(h_{(2)} \cdot b)$ for all $h \in H$ and $a, b \in B$.

(2) *If H measures B, the linear map $\sigma : H \otimes H \to B$ is called a* **cocycle** *of H with values in B if it satisfies the following two properties:*

   (a) $\sigma(h, 1) = \sigma(1, h) = \varepsilon(h)$ for all $h \in H$.

   (b) $\sum (h_{(1)} \cdot \sigma(k_{(1)}, m_{(1)}))\sigma(h_{(2)}, k_{(2)}m_{(2)}) = \sum \sigma(h_{(1)}, k_{(1)})\sigma(h_{(2)}k_{(2)}, m)$ for all $h, k, m \in H$.

(3) *If H measures B, we call B a* **twisted H-module** *(with respect to σ) if the map $H \otimes B \to B$ satisfies the following two conditions:*

   (a) $1 \cdot b = b$ for all $b \in B$.

   (b) $h \cdot (k \cdot b) = \sum \sigma(h_{(1)}, k_{(1)})(h_{(2)}k_{(2)} \cdot b)\sigma^{-1}(h_{(3)}, k_{(3)})$ for all $h, k \in H$ and $b \in B$, where here σ^{-1} denotes the convolution inverse of σ.

Definition. *Let H be a Hopf algebra, B an algebra and $\sigma : H \otimes H \to B$ a convolution invertible linear map. Furthermore, let H measure B, let σ be a cocycle, and let B be a twisted H-module with respect to σ. The* **crossed product** *$B\#_\sigma H$ is then defined to be the associative algebra with underlying vector space $B \otimes H$, identity element $1\#1$ (note that we write $b\#h$ for the element $b \otimes h \in B \otimes H$), and multiplication*

$$(a\#h)(b\#k) = \sum a(h_{(1)} \cdot b)\sigma(h_{(2)}, k_{(1)})\#h_{(3)}k_{(2)}$$

for all $a, b \in B$ and $h, k \in H$.

The algebra $B\#_\sigma H$ is in fact an H-comodule algebra via the map

$$b\#h \mapsto \sum (b\#h_{(1)}) \otimes h_{(2)}.$$

H-comodule algebras of this form are key in understanding Hopf algebra extensions, as we will now see.

Definition. *Let H be a Hopf algebra and $B \subseteq A$ an H-extension.*

(1) *The extension is called H-**cleft** if there exists a convolution invertible right H-comodule homomorphism*[32] $\gamma : H \to A$.

(2) *The extension has the (right)* **normal basis property** *if there exists an isomorphism of left B-modules and right H-comodules*[33] $A \cong B \otimes H$.

Theorem 2.2.2.4. *Let H be a Hopf algebra and $B \subseteq A$ an H-extension. The following results hold.*

(1) *The extension is H-cleft if and only if $A \cong B\#_\sigma H$.*

(2) *The extension is H-cleft if and only if it is H-Galois and has the normal basis property.*

Proof. These results can be found as Theorem 7.2.2 and Theorem 8.2.4, respectively, in [Montgomery, 1993]. □

Remark 6. *The reader can consult Proposition 7.2.3 in [Montgomery, 1993] for an explicit description of how one obtains the action of H on B and the cocycle σ from the cleftness of the extension, and Proposition 7.2.7 in the same to see how the map γ and its convolution inverse arise from a crossed product.*

2.3 Algebraic groups and their representation theory

In this section, we recall some basic facts about algebraic groups and their representation theory in positive characteristic. To that end, throughout this section G is an affine algebraic group over an algebraically closed field $\mathbb{K}$ of positive characteristic $p > 0$, unless explicitly stated otherwise.

2.3.1 Algebraic groups

Let us briefly recall what these terms mean. To each finitely-generated, commutative $\mathbb{K}$-algebra A, one can construct by a well-known process a locally-ringed space $\mathrm{Spec}(A)$. Any locally ringed space isomorphic to one obtained by such a construction is then called an **affine $\mathbb{K}$-scheme**, and these form a full subcategory of the category of locally ringed spaces. Note that this category has terminal object $\mathrm{Spec}(\mathbb{K})$.

To any affine $\mathbb{K}$-scheme X one can associate a unique finitely-generated commutative $\mathbb{K}$-algebra $\mathbb{K}[X]$ such that $X \cong \mathrm{Spec}(\mathbb{K}[X])$. In fact, there exists an anti-equivalence of categories[34]

$$\left\{\begin{matrix}\text{Finitely-generated}\\ \text{commutative } \mathbb{K}\text{-algebras}\end{matrix}\right\} \leftrightarrow \{\text{Affine } \mathbb{K}\text{-schemes}\}.$$

[32] We may always assume such γ sends 1 to 1 by rescaling if necessary.

[33] Note that B and H are both H-comodules - B as a subalgebra of A and H via the comultiplication map - so we can equip $B \otimes H$ with the structure of an H-comodule.

[34] Although we often leave it implicit, it is important to note that an affine $\mathbb{K}$-scheme by definition comes equipped with a morphism to the terminal object $\mathrm{Spec}(\mathbb{K})$; this corresponds to the $\mathbb{K}$-structure-defining inclusion of $\mathbb{K}$ into the corresponding $\mathbb{K}$-algebra.

We call $\mathbb{K}[X]$ the coordinate algebra of X. It can be identified with the $\mathbb{K}$-algebra of regular functions[35] $X \to \mathbb{A}^1$. We say that an affine $\mathbb{K}$-scheme X is **reduced** if $\mathbb{K}[X]$ has no non-zero nilpotent elements.

An **affine $\mathbb{K}$-group scheme** is then a group object in the category of affine $\mathbb{K}$-schemes. The anti-equivalence above restricts to an anti-equivalence

$$\left\{ \begin{array}{c} \text{Finitely-generated commutative} \\ \mathbb{K}\text{-Hopf algebras} \end{array} \right\} \leftrightarrow \{\text{Affine } \mathbb{K}\text{-group schemes}\}.$$

A reduced affine $\mathbb{K}$-group scheme is called an **algebraic $\mathbb{K}$-group** or an **algebraic group**.[36] One can use this anti-equivalence to derive, for a $\mathbb{K}$-group scheme G with coordinate algebra $\mathbb{K}[G]$, an equivalence

$$\{\text{Left } G - \text{modules}\} \leftrightarrow \{\text{Right } \mathbb{K}[G] - \text{comodules}\}.$$

This equivalence is the identity map on the underlying $\mathbb{K}$-vector spaces.

Furthermore, to each $\mathbb{K}$-group scheme G we can assign a $\mathbb{K}$-group functor

$$\widetilde{G} : \{\text{Commutative } \mathbb{K}\text{-algebras}\} \to \{\text{Groups}\}$$

by defining $G(R) = \mathrm{Hom}(\mathbb{K}[G], R)$ with multiplication coming from the Hopf algebra structure of $\mathbb{K}[G]$. Often we describe groups and their homomorphisms through such a functor, although it is important to note that not all such functors define a $\mathbb{K}$-group scheme. In particular, we frequently abuse notation to say, for example, "the algebraic group homomorphism $f : G \to H$ sends $g \in G$ to $f(g) \in H$" to mean "the algebraic group homomorphism $f : G \to H$ sends $g \in G(R)$ to $f(R)(g) \in H(R)$ for each commutative $\mathbb{K}$-algebra R".

An **affine subgroup scheme** of G is an affine $\mathbb{K}$-subscheme of G such that the inclusion map is a homomorphism of $\mathbb{K}$-group schemes. All closed affine subgroup schemes of G are of the form $\mathrm{Spec}(\mathbb{K}[G]/J) \hookrightarrow \mathrm{Spec}(\mathbb{K}[G])$ for a finitely-generated Hopf ideal J of $\mathbb{K}[G]$. A **normal affine subgroup scheme** of G is an affine subgroup scheme N which is preserved by the conjugation action of G on N. If a (normal) affine subgroup scheme is reduced, we simply call it a (normal) algebraic subgroup of G, or just a (normal) subgroup of G if no confusion shall arise.

2.3.2 The distribution algebra

Let us now recall the definition of the distribution algebra $\mathrm{Dist}(G)$ of a $\mathbb{K}$-group scheme G. If

$$I_1 := \{f \in \mathbb{K}[G] \mid f(1) = 0\},^{37}$$

[35]Note here that $\mathbb{A}^1 = \mathrm{Spec}(\mathbb{K}[t])$, where $\mathbb{K}[t]$ is the polynomial algebra over $\mathbb{K}$.

[36]We may sometimes also use the phrase **affine algebraic group** if we wish to emphasise the affinity.

[37]Note that this is the augmentation ideal of $\mathbb{K}[G]$, i.e. the kernel of the counit.

where we denote by 1 the identity element of $G(\mathbb{K})$, then we define

$$\mathrm{Dist}_k(G) := \{\mu : \mathbb{K}[G] \to \mathbb{K} \mid \mu \text{ is linear and } \mu(I_1^{k+1}) = 0\}$$

and

$$\mathrm{Dist}_k^+(G) = \{\mu \in \mathrm{Dist}_k(G) \mid \mu(1_{\mathbb{K}[G]}) = 0\}.$$

Note that $\mathbb{K}[G] = \mathbb{K} \oplus I_1$ and $\mathrm{Dist}_k(G) = \mathbb{K} \oplus \mathrm{Dist}_k^+(G)$. We then define

$$\mathrm{Dist}(G) := \bigcup_{k \geqslant 0} \mathrm{Dist}_k(G)$$

and

$$\mathrm{Dist}^+(G) := \bigcup_{k \geqslant 0} \mathrm{Dist}_k^+(G).$$

We equip the $\mathbb{K}$-vector space $\mathrm{Dist}(G)$ with a multiplication defined as follows: given $\mu, \rho \in \mathrm{Dist}(G)$, we define $\mu\rho$ to be the composition

$$\mathbb{K}[G] \xrightarrow{\Delta} \mathbb{K}[G] \otimes \mathbb{K}[G] \xrightarrow{\mu \otimes \rho} \mathbb{K} \otimes \mathbb{K} \xrightarrow{\sim} \mathbb{K}.$$

The multiplicative identity is the counit ε of $\mathbb{K}[G]$. This makes $\mathrm{Dist}(G)$ into a $\mathbb{K}$-algebra and $\mathrm{Dist}^+(G)$ into an ideal. If $\mu \in \mathrm{Dist}_i^+(G)$ and $\rho \in \mathrm{Dist}_j^+(G)$ one can show that[38]

$$\mu\rho \in \mathrm{Dist}_{i+j}^+(G)$$

and

$$[\mu, \rho] \in \mathrm{Dist}_{i+j-1}^+(G).$$

In other words, $\mathrm{Dist}(G)$ is a filtered algebra whose associated graded algebra is commutative. Furthermore, $\mathrm{Lie}(G)$ lies inside $\mathrm{Dist}(G)$ as $\mathrm{Dist}_1^+(G)$ and the Lie bracket on $\mathfrak{g}$ is compatible with the Lie bracket $[A, B] = AB - BA$ on $\mathrm{Dist}(G)$.

Given a morphism $\tau : G \to H$ between two $\mathbb{K}$-group schemes, one can define a linear map

$$\mathrm{Dist}(\tau) : \mathrm{Dist}(G) \to \mathrm{Dist}(H)$$

in the natural way, and if τ is in fact a homomorphism then $\mathrm{Dist}(\tau)$ is an algebra homomorphism.[39] Furthermore,[40] for affine $\mathbb{K}$-group schemes G and H, there is a $\mathbb{K}$-algebra isomorphism $\mathrm{Dist}(G \times H) \cong \mathrm{Dist}(G) \otimes \mathrm{Dist}(H)$. Putting these two facts together, it is possible to define the map

$$\mathrm{Dist}(\delta) : \mathrm{Dist}(G) \to \mathrm{Dist}(G) \otimes \mathrm{Dist}(G),$$

where $\delta : G \to G \times G$ is the diagonal morphism. If we define $\epsilon : \mathrm{Dist}(G) \to \mathbb{K}$ to be

[38] See I.7.7 in [Jantzen, 1987].
[39] See I.7.2 in [Jantzen, 1987].
[40] See I.7.4(2) and I.7.9 in [Jantzen, 1987].

map $\mu \mapsto \mu(1)$, we can prove that $(\mathrm{Dist}(G), \mathrm{Dist}(\delta), \epsilon)$ is a coalgebra.

Furthermore, we may obtain from the morphism $\iota : G \to G$ which sends g to g^{-1} the linear map

$$\mathrm{Dist}(\iota) : \mathrm{Dist}(G) \to \mathrm{Dist}(G).$$

Denoting the multiplication of $\mathrm{Dist}(G)$ by $\cdot$, one can show, for an affine $\mathbb{K}$-group scheme G, that $(\mathrm{Dist}(G), \cdot, \varepsilon, \mathrm{Dist}(\delta), \epsilon, \mathrm{Dist}(\iota))$ is a cocommutative Hopf algebra.[41]

Since $\mathfrak{g}$ embeds in $\mathrm{Dist}(G)^{(-)}$ as a Lie algebra, the universal property of $U(\mathfrak{g})$ gives a $\mathbb{K}$-algebra homomorphism

$$U(\mathfrak{g}) \to \mathrm{Dist}(G).$$

If $\mathbb{K}$ has characteristic zero,[42] this homomorphism is in fact an isomorphism. In positive characteristic, however, it is neither injective nor surjective in general. One can show that the embedding of $\mathfrak{g}$ into $\mathrm{Dist}(G)^{(-)}$ respects the p-th power maps of these Lie algebras,[43] hence we in fact obtain a $\mathbb{K}$-algebra homomorphism

$$U_0(\mathfrak{g}) \to \mathrm{Dist}(G).$$

This turns out to be injective. We shall see what the image is later on.

2.3.3 Representation theory of distribution algebras

The main reason to study the distribution algebra of a $\mathbb{K}$-group scheme is that it is better able to capture the representation theory of the algebraic group than the universal enveloping algebra $U(\mathfrak{g})$ when the field has positive characteristic. As such, it is important to understand the representation theory of distribution algebras.

Let M be a left G-module. We recall from earlier that M can be given the structure of a right $\mathbb{K}[G]$-comodule; hence, it comes equipped with a linear map $\omega : M \to M \otimes \mathbb{K}[G]$. We give M the structure of a left $\mathrm{Dist}(G)$-module as follows: given $m \in M$ and $\mu \in \mathrm{Dist}(G)$, we define μm to be the image of m under the composition

$$M \xrightarrow{\omega} M \otimes \mathbb{K}[G] \xrightarrow{id \otimes \mu} M \otimes \mathbb{K} \xrightarrow{\sim} M.$$

Furthermore, to each G-module homomorphism $f : M \to M'$ there is a natural way to construct a homomorphism of $\mathrm{Dist}(G)$-modules $M \to M'$.

Let us now recall some basic facts about the $\mathrm{Dist}(G)$-module structure of M. Proofs of all these results can be found in Chapter I.7 in [Jantzen, 1987].

Proposition 2.3.3.1. *Let G be a $\mathbb{K}$-group scheme and let M and M' be left G-*

[41]See I.7.9 in [Jantzen, 1987].

[42]It should be clear to the reader that the construction so far has not required any assumption on the characteristic of the field.

[43]As with any Lie algebra obtained from an associative algebra, $\mathrm{Dist}(G)^{(-)}$ has the structure of a (infinite-dimensional) restricted Lie algebra simply by defining the p-th power map to be the p-th power map in the underlying associative algebra.

modules.

(1) *Suppose N is a G-submodule of M. Then N is stable under the* $\mathrm{Dist}(G)$*-action on M, and so is a* $\mathrm{Dist}(G)$*-submodule of M.*

(2) *Suppose N is a G-submodule of M. Then the* $\mathrm{Dist}(G)$*-module structure of the G-module M/N is precisely that of the quotient of M by N as* $\mathrm{Dist}(G)$*-modules.*

(3) *The* $\mathrm{Dist}(G)$*-module $M \oplus M'$ is the direct sum of the* $\mathrm{Dist}(G)$*-modules M and M'.*

(4) *If $m \in M$ with $g \cdot m = m$ for all $g \in G$ then $\mu m = \mu(1)m$ for all $\mu \in \mathrm{Dist}(G)$.*

(5) *The restriction of the* $\mathrm{Dist}(G)$*-module structure of M to $\mathfrak{g} = \mathrm{Dist}_1^+(G)$ makes M into a restricted $\mathfrak{g}$-module. Furthermore, this is the same $\mathfrak{g}$-module structure as defined in Subsection 2.1.2.*

Despite this proposition, it is not true in general that there is an equivalence of categories between G-modules and $\mathrm{Dist}(G)$-modules. However, for a certain family of group schemes, such an equivalence does exist.

Definition. *An affine $\mathbb{K}$-group scheme G is called* **finite** *if $\mathbb{K}[G]$ is a finite-dimensional $\mathbb{K}$-algebra. If G is finite and the ideal $I_1 \subset \mathbb{K}[G]$ is nilpotent then G is called* **infinitesimal**.

It is clear that if G is an infinitesimal affine $\mathbb{K}$-group scheme then $\mathrm{Dist}(G) = \mathbb{K}[G]^*$.

Proposition 2.3.3.2. *Let G be a finite affine group scheme. Then the category of G-modules is equivalent to the category of* $\mathrm{Dist}(G)$*-modules.*

Proof. See Section I.8.6 in [Jantzen, 1987]. □

2.3.4 Frobenius kernels

There is a class of infinitesimal (and hence finite) group schemes which will be of particular importance in what follows. These are the so-called *Frobenius kernels* of affine $\mathbb{K}$-group schemes.

Let A be a commutative, finitely-generated $\mathbb{K}$-algebra. For $r \in \mathbb{N}$, the map[44]

$$\gamma_r : A \to A, \qquad a \mapsto a^{p^r}$$

is a ring homomorphism, but not a $\mathbb{K}$-algebra homomorphism[45] since $\gamma_r(\lambda a) = \lambda^{p^r}\gamma_r(a)$ for $a \in A$, $\lambda \in \mathbb{K}$. In order to recover a ring homomorphism, we therefore need to modify the $\mathbb{K}$-structure of A.

[44]Recall here that p is the characteristic of $\mathbb{K}$.

[45]Hence, it corresponds to a morphism of affine schemes but not of affine $\mathbb{K}$-schemes.

Definition. *Let A be a commutative, finitely-generated $\mathbb{K}$-algebra. For $r \in \mathbb{N}$, the $\mathbb{K}$-algebra $A^{(r)}$ is defined to be equal to A as a ring, but with scalar multiplication such that $\lambda \in \mathbb{K}$ acts on it as $\lambda^{p^{-r}}$ does on A.*

With this definition in mind, it is straightforward to see that γ_r induces a $\mathbb{K}$-algebra homomorphism

$$\gamma_r : A^{(r)} \to A, \qquad a \mapsto a^{p^r}.$$

We may also view this map as a $\mathbb{K}$-algebra homomorphism $A \to A^{(-r)}$. Under the anti-equivalence of categories described above, this corresponds to a morphism

$$F^r := \mathrm{Spec}(\gamma_r) : \mathrm{Spec}(A) \to \mathrm{Spec}(A^{(-r)})$$

which we call the r**-th Frobenius morphism** on $\mathrm{Spec}(A)$. Furthermore, one can check that, if A is a Hopf algebra, then the map γ_r is, in fact, a homomorphism of Hopf algebras, so F^r is a homomorphism of $\mathbb{K}$-group schemes

$$F^r : G \to G^{(r)},$$

where $G^{(r)}$ is defined to be $\mathrm{Spec}(\mathbb{K}[G]^{(-r)})$.

Definition. *If G is an affine $\mathbb{K}$-group scheme, the* r**-th Frobenius kernel** *of G is then defined to be*

$$G_r := \ker(F^r).$$

In particular, this is an affine $\mathbb{K}$-group scheme with[46]

$$\mathbb{K}[G_r] = \frac{\mathbb{K}[G]}{\sum_{f \in I_1} \mathbb{K}[G] f^{p^r}},$$

and it is a normal subgroup scheme of G. Since $I_1/(\sum_{f \in I_1} \mathbb{K}[G] f^{p^r})$ is clearly nilpotent, G_r is an infinitesimal affine $\mathbb{K}$-group scheme for all $r \in \mathbb{N}$.

The fact that we need to twist the $\mathbb{K}$-algebra structure in order to get a homomorphism is an annoyance that we can, at times, remove. We say that a commutative, finitely-generated $\mathbb{K}$-algebra A has an $\mathbb{F}_p$-form if there exists a commutative, finitely-generated $\mathbb{F}_p$-algebra A' such that $A \cong \mathbb{K} \otimes_{\mathbb{F}_p} A'$. In this case, we can define, for $r \in \mathbb{N}$, the map

$$\gamma_r^{geo} : A \to A, \qquad \lambda \otimes a \mapsto \lambda \otimes a^{p^r}.$$

This is already a homomorphism of $\mathbb{K}$-algebras (or $\mathbb{K}$-Hopf algebras, if A is a Hopf algebra), and on the level of $\mathbb{K}$-group schemes we call this the **geometric Frobenius morphism** F^r_{geo}. Furthermore, we can define, for $r \in \mathbb{N}$, the map

$$\gamma_r^{ar} : A^{(r)} \to A, \qquad \lambda \otimes a \mapsto \lambda^{p^r} \otimes a.$$

[46] Here, I_1 is as in the definition of the distribution algebra.

This map is, in fact, a $\mathbb{K}$-algebra isomorphism, which we call the **arithmetic Frobenius morphism** F_{ar}^r on the level of $\mathbb{K}$-group schemes. In particular, it is clear that $\gamma_r = \gamma_r^{geo} \circ \gamma_r^{ar}$, and we have the commutative diagram

$$\begin{tikzcd} G \arrow[r, "F_{geo}^r"] \arrow[dr, "F^r"'] & G \arrow[d, "F_{ar}^r"] \\ & G^{(r)} \end{tikzcd}$$

where the vertical arrow is an isomorphism. This implies that

$$G_r = \ker(F_{geo}^r)$$

if G is an affine $\mathbb{K}$-group scheme such that $\mathbb{K}[G]$ has an $\mathbb{F}_p$-form.[47]

Using the homomorphism $F^r : G \to G^{(r)}$ we can equip every $G^{(r)}$-module M with the structure of a G-module, which we denote by $M^{[r]}$. If G is defined over $\mathbb{F}_p$, using instead the homomorphism $F_{geo}^r : G \to G$ we may give a G-module M a "twisted" G-module structure, which we abuse notation to also denote by $M^{[r]}$. If, furthermore, M is defined over $\mathbb{F}_p$ - which is to say that there exists a subspace M' of M such that $\mathbb{K} \otimes_{\mathbb{F}_p} M' = M$ - and the representation $G \to \mathrm{GL}(M)$ is defined[48] over $\mathbb{F}_p$, then $M^{[r]} \cong M^{(r)}$ as G-modules.[49] Here $M^{(r)}$ is the $\mathbb{K}$-vector space whose underlying additive group is $(M, +)$ and such that $\lambda \in \mathbb{K}$ acts on $M^{(r)}$ as $\lambda^{p^{-r}}$ acts on M; this can be made into a G-module in a natural way.

Example 1. *The* **additive group** $\mathbb{G}_a$ *is defined to be* $\mathrm{Spec}(\mathbb{K}[t])$*. Note that the* $\mathbb{K}$*-algebra* $\mathbb{K}[t]$ *is a Hopf algebra with comultiplication defined by* $t \mapsto t \otimes 1 + 1 \otimes t$*, counit defined by* $t \mapsto 0$ *and antipode defined by* $t \mapsto -t$*. The corresponding* $\mathbb{K}$*-group functor maps a commutative* $\mathbb{K}$*-algebra* R *to the abelian group* $(R, +)$*. Given* $r \geqslant 0$*, we get the* r*-th Frobenius kernel*

$$\mathbb{G}_{a,r} = \mathrm{Spec}(\mathbb{K}[t]/\langle t^{p^r} \rangle),$$

which can also be described via the $\mathbb{K}$*-group functor*

$$R \mapsto \{x \in R \,|\, p^r x = 0\}.$$

Example 2. *The* **multiplicative group** $\mathbb{G}_m$ *is defined to be* $\mathrm{Spec}(\mathbb{K}[t, t^{-1}])$*. Note that the* $\mathbb{K}$*-algebra* $\mathbb{K}[t, t^{-1}]$ *is a Hopf algebra with comultiplication defined by* $t \mapsto t \otimes t$*, counit defined by* $t \mapsto 1$ *and antipode defined by* $t \mapsto t^{-1}$*. The corresponding* $\mathbb{K}$*-group functor maps a commutative* $\mathbb{K}$*-algebra* R *to the unit group* $(R^*, \cdot)$*. Given*

[47] We often shorten this to saying that G has an $\mathbb{F}_p$-form.

[48] The representation $\rho : G \to \mathrm{GL}_{\mathbb{K}}(M)$ is said to be **defined over** $\mathbb{F}_p$ if there is a representation $\rho' : G' \to \mathrm{GL}_{\mathbb{F}_p}(M')$ which becomes ρ under base change.

[49] See I.9.10 in [Jantzen, 1987].

$r \geqslant 0$, *we get the r-th Frobenius kernel*

$$\mathbb{G}_{m,r} = \operatorname{Spec}(\mathbb{K}[t, t^{-1}]/\langle t^{p^r} - 1\rangle),$$

which can also be described via the $\mathbb{K}$-group functor

$$R \mapsto \{x \in R^* \mid x^{p^r} = 1\}.$$

The Frobenius kernels of G form an ascending sequence

$$G_1 \subseteq G_2 \subseteq G_3 \subseteq \dots$$

of normal, infinitesimal $\mathbb{K}$-subgroup schemes of G. Applying the distribution functor, we obtain an ascending sequence

$$\operatorname{Dist}(G_1) \subseteq \operatorname{Dist}(G_2) \subseteq \operatorname{Dist}(G_3) \subseteq \dots$$

of normal Hopf subalgebras[50] of $\operatorname{Dist}(G)$. One can then show that

$$\operatorname{Dist}(G) = \bigcup_{r \geqslant 1} \operatorname{Dist}(G_r).$$

Recalling that

$$\mathfrak{g} = \operatorname{Dist}_1^+(G) = \{\mu : I_1/I_1^2 \to \mathbb{K} \mid \mu \,\text{is linear}\},$$

it is straightforward to see that $\operatorname{Lie}(G_r) := \operatorname{Dist}_1^+(G_r)$ is, in fact, equal to $\mathfrak{g}$, i.e. $\operatorname{Lie}(G_r) = \operatorname{Lie}(G)$ for all $r \in \mathbb{N}$. In particular, this means that the injective homomorphism

$$U_0(\mathfrak{g}) \hookrightarrow \operatorname{Dist}(G)$$

defined earlier is even an injective homomorphism

$$U_0(\mathfrak{g}) \hookrightarrow \operatorname{Dist}(G_1).$$

Since G_1 is infinitesimal, $\operatorname{Dist}(G_1) = \mathbb{K}[G_1]^* = \left(\mathbb{K}[G]/\left(\sum_{f \in I_1} \mathbb{K}[G]f^p\right)\right)^*$. From this, one can deduce that if $\dim(\mathfrak{g}) = n$ then $\dim \operatorname{Dist}(G_1) \leqslant p^n$. On the other hand, Proposition 2.1.3.6 shows that $\dim(U_0(\mathfrak{g})) = p^n$. Thus, there is an isomorphism

$$U_0(\mathfrak{g}) \cong \operatorname{Dist}(G_1).$$

In particular, irreducible representations of G_1 are precisely irreducible restricted representations of $\mathfrak{g}$.

Let us make a few more remarks about the structure of $\operatorname{Dist}(G_r)$.

[50] See I.7.18 and I.9.8 in [Jantzen, 1987].

Proposition 2.3.4.1. *Let G be an algebraic group over $\mathbb{K}$. Then the following results hold for $r \in \mathbb{N}$.*

(1) *The $\mathbb{K}$-dimension of* $\mathrm{Dist}(G_r)$ *is* $p^{r\dim(\mathfrak{g})}$.

(2) *The subspace* $\mathrm{Dist}_{p^r-1}(G) \subseteq \mathrm{Dist}(G)$ *is a subspace of* $\mathrm{Dist}(G_r)$.

(3) *The subalgebra of* $\mathrm{Dist}(G)$ *generated by* $\mathrm{Dist}_{p^r-1}(G)$ *is precisely* $\mathrm{Dist}(G_r)$.

Proof. For (1), see Section I.9.6 in [Jantzen, 1987]. For (2), note that if $\delta \in \mathrm{Dist}_{p^r-1}(G)$ then $\delta(I_1^{p^r}) = 0$. Hence, $\delta(\sum_{f\in I_1} \mathbb{K}[G]f^{p^r}) = 0$. Finally, (3) follows from Subsection 2.4.2, *infra.* □

Example 3. *Let $G = \mathbb{G}_a$, the additive group. Then $\mathbb{K}[G] = \mathbb{K}[t]$, the polynomial ring in one variable, and $I_1 = \langle t\rangle$. Thus,*

$$\mathrm{Dist}_n(\mathbb{G}_a) = \{\delta : \mathbb{K}[t] \to \mathbb{K} \mid \delta \textit{ is linear, and } \delta(t^k) = 0 \textit{ for all } k > n\}.$$

If we define $\gamma_i \in \mathbb{K}[t]^*$ to be the linear map with $\gamma_i(t^j) = \delta_{ij}$, then $\mathrm{Dist}_n(\mathbb{G}_a)$ *has basis $\gamma_0, \gamma_1, \ldots, \gamma_n$ and* $\mathrm{Dist}(\mathbb{G}_a)$ *has basis $\gamma_0, \gamma_1, \ldots,$ similarly. One can compute that, in* $\mathrm{Dist}(G)$*,*

$$\gamma_i\gamma_j = \binom{i+j}{i}\gamma_{i+j}$$

which implies that

$$\gamma_1^i = i!\gamma_i.$$

The reader should consult Section I.7.8 in [Jantzen, 1987] for details. In particular, this implies that, over $\mathbb{C}$, the distribution algebra $\mathrm{Dist}(\mathbb{G}_a)$ *has basis*

$$1, \gamma_1, \frac{1}{2!}\gamma_1^2, \ldots, \frac{1}{n!}\gamma_1^n \ldots$$

and it is straightforward to check that $\mathrm{Dist}(\mathbb{G}_{a,r})$ *is the subspace with basis*

$$1, \gamma_1, \frac{1}{2!}\gamma_1^2, \ldots, \frac{1}{(p^r-1)!}\gamma_1^{p^r-1}.$$

By taking the $\mathbb{Z}$-lattice $\mathrm{Dist}(\mathbb{G}_{a,\mathbb{Z}})$ *spanned by elements $\frac{1}{i!}\gamma_1^i$ for $i \geqslant 0$, we can obtain* $\mathrm{Dist}(\mathbb{G}_a)$ *over $\mathbb{K}$ as* $\mathrm{Dist}(\mathbb{G}_{a,\mathbb{Z}})\otimes_{\mathbb{Z}}\mathbb{K}$. *We then conclude that, over $\mathbb{K}$, the distribution algebra* $\mathrm{Dist}(\mathbb{G}_a)$ *has basis*

$$1\otimes 1, \gamma_1\otimes 1, \frac{1}{2!}\gamma_1^2\otimes 1, \ldots, \frac{1}{n!}\gamma_1^n\otimes 1, \ldots$$

and it is straightforward to check that $\mathrm{Dist}(\mathbb{G}_{a,r})$ *is the subspace with basis*

$$1\otimes 1, \gamma_1\otimes 1, \frac{1}{2!}\gamma_1^2\otimes 1, \ldots, \frac{1}{(p^r-1)!}\gamma_1^{p^r-1}\otimes 1.$$

Example 4. *Let $G = \mathbb{G}_m$, the multiplicative group. Then $\mathbb{K}[G] = \mathbb{K}[t, t^{-1}]$, the Laurent polynomial ring, and $I_1 = \langle t-1 \rangle$. Thus,*

$$\mathrm{Dist}_n(\mathbb{G}_a) = \{\delta : \mathbb{K}[t,t^{-1}] \to \mathbb{K} \mid \delta \textit{ is linear, and } \delta((t-1)^k) = 0 \textit{ for all } k > n\}.$$

If we define $\delta_i \in \mathbb{K}[t,t^{-1}]^*$ to be the linear map with $\delta_i((t-1)^j) = \delta_{ij}$, then $\mathrm{Dist}_n(\mathbb{G}_m)$ has basis $\delta_0, \delta_1, \ldots, \delta_n$ and $\mathrm{Dist}(\mathbb{G}_a)$ has basis $\delta_0, \delta_1, \ldots$, similarly. One can compute that, in $\mathrm{Dist}(G)$,

$$\delta_i\delta_j = \sum_{k=0}^{\min(i,j)} \frac{(i+j-k)!}{(i-k)!(j-k)!k!}\delta_{i+j-k}$$

which implies that

$$\delta_1(\delta_1 - 1)\ldots(\delta_1 - i + 1) = i!\delta_i.$$

Once again, the reader should consult Section I.7.8 in [Jantzen, 1987] for details. In particular, this implies that, over $\mathbb{C}$, the distribution algebra $\mathrm{Dist}(\mathbb{G}_a)$ has basis

$$1, \delta_1, \binom{\delta_1}{2}, \ldots, \binom{\delta_1}{n}, \ldots,$$

denoting here $\binom{\delta_1}{i} := \frac{\delta_1(\delta_1-1)\ldots(\delta_1-i+1)}{i!}$. It is straightforward to check that $\mathrm{Dist}(\mathbb{G}_{a,r})$ is the subspace with basis

$$1, \delta_1, \binom{\delta_1}{2}, \ldots, \binom{\delta_1}{p^r-1}.$$

By taking the $\mathbb{Z}$-lattice $\mathrm{Dist}(\mathbb{G}_{m,\mathbb{Z}})$ spanned by elements $\binom{\delta_1}{i}$ for $i \geqslant 0$, we can obtain $\mathrm{Dist}(\mathbb{G}_m)$ over $\mathbb{K}$ as $\mathrm{Dist}(\mathbb{G}_{m,\mathbb{Z}}) \otimes_{\mathbb{Z}} \mathbb{K}$. We then conclude that, over $\mathbb{K}$, the distribution algebra $\mathrm{Dist}(\mathbb{G}_m)$ has basis

$$1 \otimes 1, \delta_1 \otimes 1, \binom{\delta_1}{2} \otimes 1, \ldots, \binom{\delta_1}{n} \otimes 1, \ldots$$

and it is straightforward to check that $\mathrm{Dist}(\mathbb{G}_{m,r})$ is the subspace with basis

$$1 \otimes 1, \delta_1 \otimes 1, \binom{\delta_1}{2} \otimes 1, \ldots, \binom{\delta_1}{p^r-1} \otimes 1.$$

2.4 Reductive groups and their Lie algebras

The representation theory of Lie algebras in positive characteristic and of Frobenius kernels of algebraic groups is best understood in the reductive case. Let us briefly summarise the well-known structure of reductive algebraic groups and their Lie algebras, before delving into their representation theory. Much of the content of this section, including proofs of the relevant results, can be found in [Jantzen, 1987] and [Jantzen, 2004]. Throughout this section, G will be a reductive algebraic group over an algebraically closed field $\mathbb{K}$ of positive characteristic $p > 0$, and $\mathfrak{g}$ will be its

Lie algebra.

2.4.1 The structure of reductive groups and their Lie algebras

We shall call an algebraic group G **reductive** if its unipotent radical $R_u(G)$ is trivial. The unipotent radical $R_u(G)$ of G is the unique maximal connected unipotent closed normal subgroup of G, which one can show always exists. The precise definition of a unipotent subgroup of G is unimportant for this thesis, but the reader can see Chapter IV.11 in [Borel, 1991] for details.

A subgroup T of G is called a **torus** if $T \cong (\mathbb{G}_m)^d$ for some $d \in \mathbb{N}$, and is called a **maximal torus** if it is maximal with respect to his property. If $T \cong (\mathbb{G}_m)^d$ and $T' \cong (\mathbb{G}_m)^{d'}$ are two maximal tori then $d = d'$, and we call d the **rank** of G. For a maximal torus T of G we define

$$X(T) := \mathrm{Hom}(T, \mathbb{G}_m) \cong \mathbb{Z}^d$$

and we call it the **character group** of T, whose group structure we write additively. We further define the cocharacter group of T

$$Y(T) := \mathrm{Hom}(\mathbb{G}_m, T).$$

Then, as in [Jantzen, 1987, II.1.3], there exists a bilinear pairing $X(T) \times Y(T)$ given by $(\lambda, \mu) \mapsto \langle \lambda, \mu \rangle$, where $\langle \lambda, \mu \rangle$ is the integer corresponding to $\lambda \circ \mu \in \mathrm{End}(\mathbb{G}_m) = \mathbb{Z}$.

If M is a T-module, then it has a decomposition

$$M = \bigoplus_{\lambda \in X(T)} M_\lambda,$$

where

$$M_\lambda := \{m \in M \mid t \cdot m = \lambda(t)m \text{ for all } t \in T\}.$$

Since a maximal torus T acts on the Lie algebra $\mathfrak{g}$ via the adjoint action, we get a decomposition

$$\mathfrak{g} = \bigoplus_{\lambda \in X(T)} \mathfrak{g}_\lambda.$$

We call $\alpha \in X(T)$ a **root** of G with respect to T if $\alpha \neq 0$ and $\mathfrak{g}_\alpha \neq 0$, and we denote by $\Phi(G, T)$ (or just Φ if no confusion will arise) the set of roots of G with respect to T. Letting $\mathfrak{h} = \mathbb{K}^d$ be the Lie algebra of T, we get that

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in \Phi} \mathfrak{g}_\alpha.$$

For $\alpha \in \Phi$, one can show that $\mathfrak{g}_\alpha$ is one-dimensional. Since $\alpha : T \to \mathbb{G}_m$ is a homomorphism, $d\alpha : \mathfrak{h} \to \mathbb{K}$ is a linear map. We often abuse notation by using α to denote $d\alpha$, unless context would make this confusing.

To each root $\alpha \in \Phi$ one can assign a **coroot** $\alpha^\vee \in Y(T)$ in a specified way.[51] In the $\mathbb{R}$-vector space $X(T) \otimes_{\mathbb{Z}} \mathbb{R}$, the set Φ satisfies the following conditions:

(1) The $\mathbb{R}$-vector space $X(T) \otimes_{\mathbb{Z}} \mathbb{R}$ is spanned by Φ.

(2) If $\alpha \in \Phi$ then $-\alpha \in \Phi$, and if $s\alpha \in \Phi$ for $s \in \mathbb{R}$ then $s \in \{+1, -1\}$.

(3) For each $\alpha, \beta \in \Phi$, we have

$$\beta - 2\langle \beta, \alpha^\vee \rangle \alpha \in \Phi.$$

(4) For each $\alpha, \beta \in \Phi$, we have $\langle \beta, \alpha^\vee \rangle \in \mathbb{Z}$.

In other words, Φ is a **root system** in $X(T) \otimes_{\mathbb{Z}} \mathbb{R}$. In particular, this means that in Φ we can choose a system of **positive roots**, that is, a subset Φ^+ of Φ such that, for all $\alpha \in \Phi$, either $\alpha \in \Phi^+$ or $-\alpha \in \Phi^+$, and such that for all pairs $\alpha, \beta \in \Phi^+$ such that $\alpha + \beta \in \Phi$, we have $\alpha + \beta \in \Phi^+$. We define the corresponding system of **negative roots** Φ^- to be $-\Phi^+$. Inside Φ^+ we have a finite set of **simple roots** $\Pi = \{\alpha_1, \dots, \alpha_n\}$ such that no element of Π can be written as a sum of two or more elements in Φ^+. We then have that every element of Φ is of the form

$$\alpha = k_1\alpha_1 + \cdots + k_n\alpha_n$$

with $k_1, \dots, k_n \in \mathbb{Z}$; that $\alpha \in \Phi^+$ if and only if $k_1, \dots, k_n \in \mathbb{Z}_{\geqslant 0}$; and that $\alpha \in \Phi^-$ if and only if $k_1, \dots, k_n \in \mathbb{Z}_{\leqslant 0}$.

To each root $\alpha \in \Phi$ we can define a **root homomorphism**

$$x_\alpha : \mathbb{G}_a \to G$$

which satisfies $tx_\alpha(a)t^{-1} = x_\alpha(\alpha(t)a)$ for all $a \in \mathbb{G}_a$ and $t \in T$. The image of this homomorphism is a closed subgroup of G which we denote by U_α, and whose Lie algebra is $\mathfrak{g}_\alpha$. We say that a subset of Φ is unipotent if $\Psi \cap (-\Psi) = \varnothing$ and say that Ψ is closed if, for all $\alpha, \beta \in \Psi$, we have $(\mathbb{N}\alpha + \mathbb{N}\beta) \cap \Phi \subseteq \Psi$. To each closed, unipotent subset Ψ of Φ, we define $U(\Psi)$ to be the subgroup of G generated by the subgroups U_α for $\alpha \in \Psi$. In particular, we define

$$U^+ := U(\Phi^+) \qquad \text{and} \qquad U^- := U(\Phi^-).$$

We further define

$$B^+ := TU^+ \qquad \text{and} \qquad B^- := TU^-,$$

which are maximal connected solvable subgroups of G. We call B the **positive Borel subgroup**[52] of G containing T and B^- the **negative Borel subgroup** of

[51] See II.1.3 in [Jantzen, 1987] for details.

[52] Recall that a **Borel subgroup** of an algebraic group G is a maximal connected solvable subgroup.

G containing T.

Defining $\mathfrak{b}^+ = \mathrm{Lie}(B^+)$, $\mathfrak{b}^- = \mathrm{Lie}(B^-)$, $\mathfrak{n}^+ = \mathrm{Lie}(U^+)$ and $\mathfrak{n}^- = \mathrm{Lie}(U^-)$, we can show that

$$\mathfrak{n}^+ = \bigoplus_{\alpha\in\Phi^+} \mathfrak{g}_\alpha,$$

$$\mathfrak{n}^- = \bigoplus_{\alpha\in\Phi^+} \mathfrak{g}_{-\alpha},$$

and

$$\mathfrak{g} = \mathfrak{n}^- \oplus \mathfrak{h} \oplus \mathfrak{n}^-.$$

In general, we write B instead of B^+ and $\mathfrak{b}$ instead of $\mathfrak{b}^+$. We then also have

$$\mathfrak{b} = \mathfrak{h} \oplus \mathfrak{n}^+.$$

We can then choose a basis $\mathbf{h}_1, \dots, \mathbf{h}_d$ of $\mathfrak{h}$ and elements $\mathbf{e}_\alpha \in \mathfrak{g}_\alpha$ for $\alpha \in \Phi$ such that

$$\{\mathbf{e}_\alpha,\, \mathbf{h}_t \mid \alpha \in \Phi,\, 1 \leqslant t \leqslant d\}$$

is a basis of $\mathfrak{g}$. Defining $\mathbf{h}_\alpha = [\mathbf{e}_{-\alpha}, \mathbf{e}_\alpha]$, these satisfy the following relations:

(1) $[h, k] = 0$ for all $h, k \in \mathfrak{h}$.

(2) $[h, \mathbf{e}_\alpha] = \alpha(h)\mathbf{e}_\alpha$ for all $h \in \mathfrak{h}$ and $\alpha \in \Phi$.

(3) $[\mathbf{e}_{-\alpha}, \mathbf{e}_\alpha] = \mathbf{h}_\alpha$ can be written as a $\mathbb{Z}$-linear combination of $\mathbf{h}_1, \dots, \mathbf{h}_d$.

(4) $[\mathbf{e}_\alpha, \mathbf{e}_\beta] = \pm(m+1)\mathbf{e}_{\alpha+\beta}$ for $\alpha \neq -\beta \in \Phi$, where $m = \max\{k \in \mathbb{N} \mid \beta - k\alpha \in \Phi\}$ and $\mathbf{e}_{\alpha+\beta} := 0$ if $\alpha + \beta \notin \Phi$.

The basis $\{\mathbf{e}_\alpha,\, \mathbf{h}_t \mid \alpha \in \Phi,\, 1 \leqslant t \leqslant d\}$ is called a **Chevalley basis** of $\mathfrak{g}$.[53] Furthermore, it is not difficult to see, viewing the elements of $\mathfrak{g}$ as derivations of $\mathbb{K}[G]$, that $\mathbf{e}_\alpha^{[p]} = 0$ for $\alpha \in \Phi$ and $\mathbf{h}_t^{[p]} = \mathbf{h}_t$ for all $1 \leqslant t \leqslant d$. This demonstrates the p-structure on $\mathfrak{g}$.

A (reductive) algebraic group is called **semisimple** if it contains no non-trivial solvable connected closed normal subgroups. This is equivalent to the condition that $\mathbb{Z}\Phi$ has finite index in $X(T)$. A semisimple algebraic group is called **simply-connected** if $Y(T) = \mathbb{Z}\Phi^\vee = \mathbb{Z}\{\alpha^\vee \mid \alpha \in \Phi\}$. See [Jantzen, 1987, I.1.6] for more details.

2.4.2 Divided powers

For a Hopf algebra H, we define the set of primitive elements

$$P(H) := \{x \in H \mid \Delta(x) = x \otimes 1 + 1 \otimes x\},$$

[53]See, for example, Chapter VII in [Humphreys, 1972] for a discussion of the characteristic zero case.

and the set of group-like elements

$$G(H) := \{x \in H \mid \Delta(x) = x \otimes x\}.$$

Given an element $x \in P(H)$, a sequence $x^{(0)}, x^{(1)}, x^{(2)}, \ldots, x^{(k)} \in H$ is said to be a **sequence of divided powers** of x if

(1) $x^{(0)} = 1$.

(2) $x^{(1)} = x$.

(3) $\Delta(x^{(l)}) = \sum_{i=0}^{l} x^{(i)} \otimes x^{(l-i)}$ for all $l \geqslant 0$.

Suppose that $x_1, \ldots, x_n$ is a basis for the Lie algebra $\mathfrak{g} = \mathrm{Lie}(G)$, where G is an affine algebraic group. For each $1 \leqslant i \leqslant n$, there exists an infinite sequence of divided powers $x_i^{(0)}, x_i^{(1)}, x_i^{(2)}, \ldots$ of x_i in the cocommutative Hopf algebra $\mathrm{Dist}(G)$. It is well-known[54] that the distribution algebra $\mathrm{Dist}(G_r)$ has basis

$$\{x_1^{(a_1)} x_2^{(a_2)} \ldots x_n^{(a_n)} \mid 0 \leqslant a_i < p^r \text{ for all } 1 \leqslant i \leqslant n\},$$

while the vector space $\mathrm{Dist}_k(G)$ has basis

$$\left\{ x_1^{(a_1)} x_2^{(a_2)} \ldots x_n^{(a_n)} \,\middle|\, \sum_{i=1}^{n} a_i \leqslant k \right\}.$$

One can also observe that $x_i^{(k)} \in \mathrm{Dist}_k(G)$ for all $1 \leqslant i \leqslant n$ and $k \in \mathbb{N}$.

In particular, if G is a reductive algebraic group with $\mathrm{Lie}(G) = \mathfrak{g}$, we saw in Subsection 2.4.1 that $\mathfrak{g}$ has a basis consisting of elements $\mathbf{e}_\alpha$ for $\alpha \in \Phi$ and $\mathbf{h}_t$ for $1 \leqslant t \leqslant d$. To define a basis for $\mathrm{Dist}(G)$, we hence would like to construct a sequence of divided powers for these basis elements. To do this, we first need to work over $\mathbb{C}$.

Define $G_{\mathbb{C}}$ to be the simply-connected reductive algebraic group with the same rank and same root system of G. If we define by $\mathfrak{g}_{\mathbb{C}}$ the $\mathbb{C}$-Lie algebra of $G_{\mathbb{C}}$, then $\mathfrak{g}_{\mathbb{C}}$ also has a $\mathbb{C}$-basis consisting of elements $\mathbf{e}_\alpha$ for $\alpha \in \Phi$ and $\mathbf{h}_t$ for $1 \leqslant t \leqslant d$. Further defining $\mathfrak{g}_{\mathbb{Z}}$ to be the $\mathbb{Z}$-span of these basis elements in $\mathfrak{g}_{\mathbb{C}}$, we obtain that $\mathfrak{g} = \mathfrak{g}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{K}$. We abuse notation by using $\mathbf{e}_\alpha$ and $\mathbf{h}_t$ for both the elements in $\mathfrak{g}_{\mathbb{C}}$ and the corresponding elements in $\mathfrak{g}$.

In $U(\mathfrak{g}_{\mathbb{C}})$, which is a cocommutative Hopf algebra, we define sequences of divided powers for these elements as follows. Given $\alpha \in \Phi$ and $k \in \mathbb{N}$, we define

$$\mathbf{e}_\alpha^{(k)} := \frac{\mathbf{e}_\alpha^k}{k!},$$

and, given $1 \leqslant t \leqslant d$ and $k \in \mathbb{N}$, we define

$$\binom{\mathbf{h}_t}{k} := \frac{\mathbf{h}_t(\mathbf{h}_t - 1) \ldots (\mathbf{h}_t - k + 1)}{k!}.$$

[54]See [Sweedler, 1967].

It is shown in [Kostant, 1966] and [Jantzen, 1987, II.1.12] that the set

$$\widetilde{U}(\mathfrak{g})_{\mathbb{Z}} = \mathbb{Z}\left\{ \prod_{\alpha\in\Phi^+} \mathbf{e}_{\alpha}^{(i_\alpha)} \prod_{t=1}^{d} \binom{\mathbf{h}_t}{k_t} \prod_{\alpha\in\Phi^+} \mathbf{e}_{-\alpha}^{(j_\alpha)} \quad \middle| \quad i_\alpha, j_\alpha, k_t \geqslant 0 \right\}$$

is a $\mathbb{Z}$-form for $U(\mathfrak{g}_{\mathbb{C}})$, and that

$$\mathrm{Dist}(G) = \widetilde{U}(\mathfrak{g})_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{K}.$$

In particular, this gives us a $\mathbb{K}$-basis of $\mathrm{Dist}(G)$ for reductive groups. We once again abuse notation to denote by $\mathbf{e}_{\alpha}^{(k)}$ and $\binom{\mathbf{h}_t}{k}$ the corresponding basis elements in both $U(\mathfrak{g}_{\mathbb{C}})$ and $\mathrm{Dist}(G)$.

2.4.3 Representations of reductive Lie algebras

With this set-up, let us now discuss the representation theory of the reductive Lie algebra $\mathfrak{g}$. For the remainder of this section we assume $\chi \in \mathfrak{g}^*$ vanishes on $\mathfrak{n}^+$. An argument in [Kac and Weisfeiler, 1976] shows that this assumption holds if, for example, the derived group of G is simply-connected.[55]

Let $\lambda \in \mathfrak{h}^*$. We define a 1-dimensional (irreducible) $\mathfrak{b}$-module $\mathbb{K}_\lambda$ by making $\mathfrak{n}^+$ act as 0 and $\mathfrak{h}$ act via λ. This $\mathfrak{b}$-module extends to a $U_\chi(\mathfrak{b})$-module if and only if

$$\lambda \in \Lambda_\chi := \{\lambda \in \mathfrak{h}^* \mid \lambda(h)^p - \lambda(h^{[p]}) = \chi(h)^p \text{ for all } h \in \mathfrak{h}\}.$$

This is equivalent to the requirement that $\lambda(\mathbf{h}_t)^p - \lambda(\mathbf{h}_t) = \chi(\mathbf{h}_t)^p$ for all $1 \leqslant t \leqslant d$, and hence $|\Lambda_\chi| = p^{\dim(\mathfrak{h})}$.

Given $\lambda \in \Lambda_\chi$ we can then define the **baby Verma module**

$$Z_\chi(\lambda) := U_\chi(\mathfrak{g}) \otimes_{U_\chi(\mathfrak{b})} \mathbb{K}_\lambda.$$

This is a finite-dimensional $U_\chi(\mathfrak{g})$-module of dimension $p^{\dim(\mathfrak{n}^-)}$. It has as basis the set

$$\left\{ \left(\prod_{\alpha\in\Phi^+} \mathbf{e}_{-\alpha}^{k_\alpha} \right) \otimes 1 \mid 0 \leqslant k_\alpha < p \right\},$$

where we have fixed an order of the positive roots in Φ.

Proposition 2.4.3.1. *Every irreducible $U_\chi(\mathfrak{g})$-module is a quotient of a baby Verma module $Z_\chi(\lambda)$ for some $\lambda \in \Lambda_\chi$.*

Proof. By Frobenius reciprocity it is enough to show that every $U_\chi(\mathfrak{b})$-module is of the form $\mathbb{K}_\lambda$ for some $\lambda \in \Lambda_\chi$. This follows from B.3 in [Jantzen, 2004]. $\square$

We also have the following result, which gives information about the dimensions of $U_\chi(\mathfrak{g})$-modules. It was first conjectured in [Kac and Weisfeiler, 1971] and

[55] Recall that the derived group of a connected reductive algebraic group is semisimple.

then proved in [Premet, 1995]. The paper [Premet and Skryabin, 1999] contains an alternative proof.

Theorem 2.4.3.2 (Premet's Theorem)**.** *Suppose that the derived group of G is simply-connected, that the prime p is good for $\mathfrak{g}$,*[56] *and that $\mathfrak{g}$ is equipped with a non-degenerate G-invariant bilinear form. Then, for any $U_\chi(\mathfrak{g})$-module V, the dimension of V is divisible by $p^{\dim(G\cdot\chi)/2}$.*

This structure is, in fact, already enough to classify the irreducible $\mathfrak{sl}_2$-modules in most cases. It is well-known[57] that each element of $\mathfrak{sl}_2^*$ is conjugate under the adjoint SL_2-action to a linear form such that

$$\mathbf{e} \mapsto 0 \qquad \mathbf{f} \mapsto 0 \qquad \mathbf{h} \mapsto t,$$

where $t \in \mathbb{K}$, or

$$\mathbf{e} \mapsto 0 \qquad \mathbf{f} \mapsto 1 \qquad \mathbf{h} \mapsto 0.$$

Here we are using the standard notation of $\mathbf{e}, \mathbf{h}, \mathbf{f} \in \mathfrak{sl}_2$ to mean

$$\mathbf{e} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad \mathbf{h} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \mathbf{f} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

A linear form conjugate to the first type is called **semisimple**, and a linear form conjugate to the second type (or 0) is called **nilpotent**. Using Proposition 2.1.3.7, a classification of $U_\chi(\mathfrak{sl}_2)$-modules simply requires a classification for χ non-zero semisimple, χ non-zero nilpotent, and $\chi = 0$.

Theorem 2.4.3.3. *Let $\mathbb{K}$ be an algebraically closed field of characteristic $p > 2$,*[58] *and let $\chi \in \mathfrak{sl}_2^*$. Then the following results hold.*

(1) *If $\chi \neq 0$ is semisimple, then the irreducible $U_\chi(\mathfrak{sl}_2)$-modules are precisely the baby Verma modules $Z_\chi(\lambda)$ for $\lambda \in \Lambda_\chi$. Furthermore, if $\lambda, \mu \in \Lambda_\chi$ then $Z_\chi(\lambda) \cong Z_\chi(\mu)$ if and only if $\lambda = \mu$.*

(2) *If $\chi \neq 0$ is semisimple, then the irreducible $U_\chi(\mathfrak{sl}_2)$-modules are precisely the baby Verma modules $Z_\chi(\lambda)$ for $\lambda \in \Lambda_\chi$. In this case, $\Lambda_\chi = \mathbb{F}_p$. Furthermore, if $\lambda, \mu \in \Lambda_\chi$ then $Z_\chi(\lambda) \cong Z_\chi(\mu)$ if and only if $\lambda = p - \mu - 2$.*

(3) *If $\chi = 0$, then every baby Verma module $Z_0(\lambda)$ for $\lambda \in \Lambda_0$ has a unique irreducible quotient and every irreducible $U_0(\mathfrak{sl}_2)$-module appears in this way. Furthermore, if the irreducible quotients of $Z_0(\lambda)$ and $Z_0(\mu)$ for $\lambda, \mu \in \Lambda_0$ are isomorphic, then $\mu = \lambda$.*

Proof. See Section 5 in [Jantzen, 1997]. □

[56] A prime p being good for $\mathfrak{g}$ is a property of the root system, and specifically means that: $p \neq 2$ for types B_n ($n \geqslant 2$), C_n ($n \geqslant 2$), or D_n ($n \neq 4$); $p \neq 2, 3$ for types E_6, E_7, F_4 or G_2; and $p \neq 2, 3, 5$ for type E_8.

[57] See, for example, Section 5.4 in [Jantzen, 1997].

[58] The reader can consult Section 5.6 in [Jantzen, 1997] to see what happens in characteristic 2.

2.4.4 Representations of reductive groups and their Frobenius kernels

We may also derive representation-theoretic results about the Frobenius kernels G_r for $r \geqslant 1$. Since irreducible representations of G_1 correspond to irreducible restricted representations of $\mathfrak{g}$, some analogies can be seen between these approaches.

Note that for an algebraic group G with $\mathbb{K}$-subgroup scheme H, there is a functor

$$\mathrm{Ind}_H^G : \mathrm{Mod}(H) \to \mathrm{Mod}(G)$$

which is right adjoint to the restriction functor

$$\mathrm{Res}_H^G : \mathrm{Mod}(G) \to \mathrm{Mod}(H).$$

More details on the construction can be found in Chapter I.3 in [Jantzen, 1987].

We define

$$X(T)_+ := \{\lambda \in X(T) | \langle \lambda, \alpha^\vee \rangle \geqslant 0 \text{ for all } \alpha \in \Pi\}$$

to be the set of **dominant weights** of T with respect to Φ^+ and, for $r \geqslant 1$, we set

$$X_r(T) := \{\lambda \in X(T) | \, 0 \leqslant \langle \lambda, \alpha^\vee \rangle < p^r \text{ for all } \alpha \in \Pi\}.$$

We often make the assumption that the abelian group $X(T)/p^r X(T)$ has a set of representatives $X_r'(T)$ with $X_r'(T) \subseteq X_r(T)$. We call this Assumption (R). This holds if, for example, G is semisimple and simply-connected. Furthermore, any reductive group G has a covering group $\widetilde{G}$ which satisfies Assumption (R), although it need not be the case that $\widetilde{G}_r$ is a covering group of G_r. The reader can consult II.1.17 and II.3.15 in [Jantzen, 1987] for more details.

Remark 7. *Assumption (R) fails, for example, for $G = \mathrm{PGL}_2$. This has root system $A_1 = \{\alpha, -\alpha\}$. Observe that*

$$\mathbb{Z} \xrightarrow{\sim} X(T), \quad \textit{where} \quad n \mapsto \left(\lambda_n : \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} \mapsto a^n\right)$$

and

$$\mathbb{Z} \xrightarrow{\sim} Y(T), \quad \textit{where} \quad n \mapsto \left(\mu_n : a \mapsto \begin{bmatrix} a^n & 0 \\ 0 & 1 \end{bmatrix}\right),$$

using square brackets to denote the image of a matrix in PGL_2. Furthermore, observe that the natural map $\phi_\alpha : \mathrm{SL}_2 \to \mathrm{PGL}_2$ induces the coroot

$$\alpha^\vee : a \mapsto \begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} = \begin{bmatrix} a^2 & 0 \\ 0 & 1 \end{bmatrix}.$$

Thus, $\langle \lambda_n, \alpha^\vee \rangle = 2n$ for any $n \in \mathbb{Z}$ and so, using the above identifications, $X_r(T) = \{\lambda_n \,|\, 0 \leqslant 2n < p^r\}$. In particular, taking p odd and $n = \frac{p^r+1}{2}$, we obtain that $\langle \lambda_n + p^r\lambda_m, \alpha^\vee \rangle = p^r + 1 + 2p^r m$ for any $m \in \mathbb{Z}$. Hence, $\lambda_n + p^r\lambda_m \notin X_r(T)$ for any $m \in \mathbb{Z}$, and so $X(T)/p^rX(T)$ does not have a system of representatives in $X_r(T)$.

We then define, for $\lambda \in X(T)$,

$$\nabla(\lambda) \coloneqq \mathrm{Ind}_B^G(\mathbb{K}_\lambda),$$

where $\mathbb{K}_\lambda$ is the 1-dimensional $B = TU^+$-module on which U^+ acts trivially and T acts via λ. Similarly, for $r \geqslant 1$ and $\lambda \in X(T)$ we define

$$\nabla_r(\lambda) \coloneqq \mathrm{Ind}_{B_r}^{G_r}(\mathbb{K}_\lambda),$$

where B_r is the r-th Frobenius kernel of B.

Theorem 2.4.4.1. *Keep the notation from above.*

(1) *Let M be a G-module. Then M is irreducible if and only if M is isomorphic to*
$$L(\lambda) \coloneqq \mathrm{soc}_G \nabla(\lambda)$$
for some $\lambda \in X(T)_+$.[59] *Furthermore, given $\lambda, \mu \in X(T)_+$, $L(\lambda) \cong L(\mu)$ if and only if $\lambda = \mu$.*

(2) *Let M be a G_r-module. Then M is irreducible if and only if M is isomorphic to*
$$L_r(\lambda) \coloneqq \mathrm{soc}_{G_r} \nabla_r(\lambda)$$
for some $\lambda \in X(T)_+$. Furthermore, given $\lambda, \mu \in X(T)_+$, we have $L_r(\lambda) \cong L_r(\mu)$ if and only if $\lambda - \mu \in p^rX(T)$.

Proof. Statement 1 follows from Corollary II.2.3, Proposition II.2.4 and Proposition II.2.6 in [Jantzen, 1987]. Statement 2 follows from II.3.9(2) and Proposition II.3.10 in [Jantzen, 1987]. □

Proposition 2.4.4.2. *Keep the notation from above, and let $\lambda \in X_r(T) \subseteq X(T)$. Then $\mathrm{Res}_{G_r}^G L(\lambda)$ is an irreducible G_r-module, and is isomorphic to $L_r(\lambda)$.*

Proof. This is Proposition II.3.15 in [Jantzen, 1987]. □

Remark 8. *Combining these two propositions shows that if Assumption (R) is satisfied, then every irreducible G_r-module extends to an irreducible G-module. In particular, if we consider the irreducible G_r-module $L_r(\lambda)$ for $\lambda \in X(T)_+$ then Assumption (R) says that there exists $\mu \in X_r'(T) \subseteq X_r(T)$ such that $\lambda - \mu \in p^rX(T)$. Hence $L_r(\lambda) \cong L_r(\mu)$ as G_r-modules, and Proposition 2.4.4.2 says that $L_r(\mu) \cong L(\mu)$ as*

[59] Recall that the socle of a module is the sum of its irreducible submodules.

G_r-modules. But $L(\mu)$ is also an irreducible G-module, so $L_r(\lambda)$ has been successfully extended to an irreducible G-module.

Proposition 2.4.4.3. *Let $\lambda \in X_r(T)$ and $\mu \in X(T)_+$. Then there is an isomorphism of G-modules*

$$L(\lambda + p^r\mu) \cong L(\lambda) \otimes L(\mu)^{[r]}.$$

Proof. See Proposition II.3.16 in [Jantzen, 1987]. □

This leads immediately to Steinberg's tensor product theorem.

Corollary 2.4.4.4 (Steinberg's Tensor Product Theorem)**.** *Let $\lambda_0, \lambda_1, \ldots, \lambda_r \in X_1(T)$. Set $\lambda = \sum_{i=0}^{r} p^i \lambda_i \in X(T)_+$. Then there is an isomorphism of G-modules*

$$L(\lambda) \cong L(\lambda_0) \otimes L(\lambda_1)^{[1]} \otimes \cdots \otimes L(\lambda_r)^{[r]}.$$

Proof. See Section II.3.17 in [Jantzen, 1987]. □

Chapter 3

Higher Deformations - Constructions

Let G be an algebraic group over an algebraically closed field $\mathbb{K}$ of characteristic $p > 0$ with Lie algebra $\mathfrak{g}$. We saw in Subsection 2.3.4 that $U_0(\mathfrak{g}) \cong \mathrm{Dist}(G_1)$ and that every irreducible representation of $\mathfrak{g}$ is an irreducible $U_\chi(\mathfrak{g})$-module for some $\chi \in \mathfrak{g}^*$. At the end of [Friedlander and Parshall, 1990], the authors pose the following question, posed to them in turn by Humphreys:

"**Hyperalgebra analogues.** *Do the algebras $U_\chi(\mathfrak{g})$ have natural analogues corresponding to the infinitesimal group schemes G_r associated to G for $r > 1$?*"

This chapter answers the question in the affirmative. We begin by observing that this question has been previously considered from a different perspective - namely, the theory of differential operators.

3.1 Differential operators

3.1.1 Sheaves of differential operators

Before getting into the substance of this chapter, let us consider a slightly different perspective on the topic at hand. While not directly considering the question of Friedlander and Parshall, some other authors have considered higher generalizations of the universal enveloping algebra, through the lens of differential operators. It is worthwhile summarising what is known in this case before we delve into our new constructions.

When studying sheaves of differential operators on a smooth variety X over an algebraically closed field $\mathbb{K}$ of positive characteristic there are several distinct notions, which coincide in zero characteristic. Firstly, there are the differential operators constructed by Grothendieck. The precise construction is omitted here, but the reader should consult [Dieudonné and Grothendieck, 1960–67] for more detail. In particular, the sheaf $\mathcal{D}iff_{X/\mathbb{K}}$ of these differential operators lies inside the sheaf $\mathcal{E}nd_{\mathbb{K}}(\mathcal{O}_X)$.

This sheaf has a filtration

$$\mathcal{D}^{(0)}_{X/\mathbb{K}} \to \mathcal{D}^{(1)}_{X/\mathbb{K}} \to \ldots \to \mathcal{D}^{(m)}_{X/\mathbb{K}} \to \ldots \to \mathcal{D}iff_{X/\mathbb{K}} = \varinjlim \mathcal{D}^{(m)}_{X/\mathbb{K}}$$

constructed in [Berthelot, 1996]. The sheaf $\mathcal{D}^{(0)}_{X/\mathbb{K}}$ is called the sheaf of **crystalline differential operators** and was constructed by Berthelot before the rest of the filtration was developed. This sheaf is used by Bezrukavnikov, Mirković and Rumynin in [Bezrukavnikov et al., 2008] where they use it to derive a version of Beilinson-Bernstein's localisation theorem in positive characteristic. The sheaves $\mathcal{D}^{(m)}_{X/\mathbb{K}}$ are called the sheaves of **arithmetic differential operators**.

When $X = G$ is a smooth algebraic group we can compare the sheaves of differential operators with the universal enveloping algebra of $\mathrm{Lie}(G)$ and the distribution algebra $\mathrm{Dist}(G)$. In particular, there is an injective algebra homomorphism $\mathrm{Dist}(G) \hookrightarrow \Gamma(G, \mathcal{D}iff_{G/\mathbb{K}})$, which is an isomorphism onto the subalgebra of left invariant differential operators.[60] Similarly, there is an injective algebra homomorphism $U(\mathfrak{g}) \hookrightarrow \Gamma(G, \mathcal{D}^{(0)}_{X/\mathbb{K}})$ which is an isomorphism onto the left invariant crystalline differential operators.

In trying to construct the analogues to the $U_\chi(\mathfrak{g})$ from Friedlander and Parshall's question, one sees that the arithmetic differential operators should play a role. To work with arithmetic differential operators explicitly, it helps to recall from [Hashimoto et al., 2006] that

$$\mathcal{D}^{(m)}_{X/\mathbb{K}} \cong \frac{T_{\mathbb{K}}(\mathcal{D}iff^{2p^m-1})}{\left\langle \begin{array}{c} \lambda - \lambda 1_{\mathcal{O}_X},\ \delta\otimes\delta' - \delta'\otimes\delta - [\delta,\delta'],\ \delta\otimes\delta'' - \delta\delta'' \\ \text{where } \lambda\in\mathbb{K},\ \delta''\in\mathcal{D}iff^{p^m-1},\ \delta,\delta'\in\mathcal{D}iff^{p^m} \end{array} \right\rangle},$$

where we denote by $\mathcal{D}iff^k$ the sheaf of differential operators of order $\leqslant k$.

Motivated by this, Kaneda and Ye[61] define the algebra

$$\mathbb{U}^{(m)} := \frac{T_{\mathbb{K}}(\mathrm{Dist}_{2p^m-1}(G))}{\left\langle \begin{array}{c} \lambda - \lambda\varepsilon_G,\ \delta\otimes\delta' - \delta'\otimes\delta - [\delta,\delta'],\ \delta\otimes\delta'' - \delta\delta'' \\ \text{where } \lambda\in\mathbb{K},\ \delta''\in\mathrm{Dist}_{p^m-1}(G),\ \delta,\delta'\in\mathrm{Dist}_{p^m}(G) \end{array} \right\rangle},$$

with ε_G the counit of $\mathbb{K}[G]$. They obtain, when G is reductive, the following commutative diagram of $\mathbb{K}[G]$-modules:[62]

$$\begin{array}{ccc} \mathbb{K}[G]\otimes_{\mathbb{K}}\mathbb{U}^{(m)} & \xrightarrow{\sim} & \Gamma(G,\mathcal{D}^{(m)}_{X/\mathbb{K}}) \\ \downarrow & & \downarrow \\ \mathbb{K}[G]\otimes_{\mathbb{K}}\mathrm{Dist}(G) & \xrightarrow{\sim} & \Gamma(G,\mathcal{D}iff_{G/\mathbb{K}}) \end{array}$$

[60] See I.7.18 in [Jantzen, 1987] for details.
[61] See Section 1.2 in [Kaneda and Ye, 2007].
[62] See Corollary 1.5 in [Kaneda and Ye, 2007].

with $\varinjlim \mathbb{U}^{(m)} \cong \mathrm{Dist}(G)$.

To answer Friedlander and Parshall's question we need a slightly different presentation of this algebra. We see in Subsection 3.4.2, *infra*, that the later construction gives an algebra isomorphic to $\mathbb{U}^{(m)}$.

3.2 The algebra $U^{[r]}(G)$

3.2.1 Filtered algebras

Before we get to the construction of the algebras $U^{[r]}(G)$ that we will be studying in this chapter, let us generalise slightly the situation we are considering so that we can develop some notation and tools to work with in our particular circumstance. Suppose that A is a filtered Hopf algebra[63] $A = \bigcup_{k\in\mathbb{N}} A_k$ with $A_0 = \mathbb{K}$ and such that the associated graded algebra $\mathrm{gr}(A) := \bigoplus_{k\in\mathbb{N}} A_{k+1}/A_k$ is commutative.[64] We denote $A_k^+ := A_k \cap \ker(\varepsilon_A)$, where ε_A is the counit of A.

We can construct the algebra

$$U^{[k]}(A) := \frac{T(A_k^+)}{Q_k},$$

where Q_k is the two-sided ideal generated by the relations:

(i) $x \otimes y = xy$ if $x \in A_i^+$, $y \in A_j^+$ with $i + j < k + 1$, and

(ii) $x \otimes y - y \otimes x = [x, y]$ if $x \in A_i^+$, $y \in A_j^+$ with $i + j \leqslant k + 1$.

Definition. *Let A be a filtered Hopf algebra $A = \bigcup_{k\in\mathbb{N}} A_k$ satisfying the above conditions, and B a $\mathbb{K}$-algebra. We will call a $\mathbb{K}$-linear map $\phi : A_k^+ \to B$ an* **indexed algebra subspace homomorphism** *if $\phi(xy) = \phi(x)\phi(y)$ for all $x \in A_i^+$ and $y \in A_j^+$ with $i + j < k + 1$, and $\phi([x, y]) = [\phi(x), \phi(y)]$ for all $x \in A_i^+$ and $y \in A_j^+$ with $i + j \leqslant k + 1$.*

There is a natural indexed algebra subspace homomorphism $\iota_Q : A_k^+ \to U^{[k]}(A)$.

Definition. *Let A be a filtered Hopf algebra $A = \bigcup_{k\in\mathbb{N}} A_k$ satisfying the above conditions. The* **indexed algebra subspace dual** *of A_k^+ is the set of all indexed algebra subspace homomorphisms from A_k^+ to $\mathbb{K}$. We denote it by $(A_k^+)^{\overline{*}}$.*

It is straightforward to prove the following universal property:

Proposition 3.2.1.1. *Let A be a filtered Hopf algebra $A = \bigcup_{k\in\mathbb{N}} A_k$ satisfying the above conditions, and B a $\mathbb{K}$-algebra. Let $\phi : A_k^+ \to B$ be an indexed algebra subspace homomorphism. Then there exists a unique algebra homomorphism $\overline{\phi} : U^{[k]}(A) \to B$ such that $\overline{\phi} \circ \iota_Q = \phi$.*

[63] A Hopf algebra A is called a **filtered Hopf algebra** if it is equipped with a set $\{A_k\}_{k\in\mathbb{N}}$ of subspaces of A such that $A_k \subseteq A_{k+1}$ for all $k \in \mathbb{N}$, $A = \bigcup_{k\in\mathbb{N}} A_k$, and, for all $k, l \in \mathbb{N}$, $A_k A_l \subseteq A_{k+l}$, $\Delta(A_k) \subseteq \sum_{i=0}^{k} A_i \otimes A_{k-i}$, and $S(A_k) \subseteq A_k$.

[64] In other words, $[A_k, A_l] \subseteq A_{k+l-1}$ for all k, l.

Let $\widehat{U}^{[k]}(A)$ be the algebra constructed in the same way as $U^{[k]}(A)$ except using A_i instead of A_i^+ for $i \in \mathbb{N}$ whenever relevant. This has a similar universal property, and using the universal properties for the linear maps $A_k^+ \hookrightarrow A_k$ and $A_k \to \mathbb{K} \oplus A_k^+$ it can be shown that the algebras $\widehat{U}^{[k]}(A)$ and $U^{[k]}(A)$ are isomorphic.[65] We abuse notation to refer to both algebras as $U^{[k]}(A)$.

Corollary 3.2.1.2. *Let A be a filtered Hopf algebra $A = \bigcup_{k\in\mathbb{N}} A_k$ satisfying the above conditions. Then $U^{[k]}(A)$ is a Hopf algebra for all $k \geqslant 0$. Furthermore, if A is cocommutative then $U^{[k]}(A)$ is cocommutative.*

Proof. We already know that $U^{[k]}(A)$ is an associative algebra. Applying Proposition 3.2.1.1 to the comultiplication and counit maps on the coalgebra A_k constructs the comultiplication and counit maps on $U^{[k]}(A)$. Furthermore, the antipode on A sends A_k to A_k and so we get the antipode on $U^{[k]}(A)$ from Proposition 3.2.1.1. It is straightforward to check that the Hopf algebra axioms hold, and similarly straightforward to show cocommutativity when A is cocommutative. $\square$

Definition. *Let A be a filtered Hopf algebra $A = \bigcup_{k\in\mathbb{N}} A_k$ satisfying the above conditions. An* **indexed algebra subspace representation** *of A_k^+ is an indexed algebra subspace homomorphism $\phi : A_k^+ \to \mathrm{End}(M)$ where M is a $\mathbb{K}$-vector space.*

Definition. *Let A be a filtered Hopf algebra $A = \bigcup_{k\in\mathbb{N}} A_k$ satisfying the above conditions. A $\mathbb{K}$-vector space M is called an* **indexed A_k^+-module** *if there exists an indexed algebra subspace homomorphism $\theta : A_k^+ \to \mathrm{End}(M)$. For $a \in A_k^+$ and $m \in M$ we often write $a \cdot m$ or just am for the element $\theta(a)(m)$.*

Definition. *Let A be a filtered Hopf algebra $A = \bigcup_{k\in\mathbb{N}} A_k$ satisfying the above conditions, and let $(M_1, \theta_1), (M_2, \theta_2)$ be indexed A_k^+-modules. A* **homomorphism of indexed A_k^+-modules** *is a linear map $\phi : M_1 \to M_2$ such that $\phi(am) = a\phi(m)$ for all $a \in A_k^+$ and $m \in M$.*

We can use the universal property in a standard way to get the following theorem.

Proposition 3.2.1.3. *There is a bijection between the set of (isomorphism classes of) indexed A_k^+-modules and the set of (isomorphism classes of) $U^{[k]}(A)$-modules.*

3.2.2 Higher universal enveloping algebras

Observe that, for an affine algebraic group G, the distribution algebra $\mathrm{Dist}(G)$ is a filtered Hopf algebra[66] $\mathrm{Dist}(G) = \bigcup_{k\in\mathbb{N}} \mathrm{Dist}_k(G)$ with $\mathrm{Dist}_0(G) = \mathbb{K}$, such that the associated graded algebra

$$\mathrm{gr}(\mathrm{Dist}(G)) = \bigoplus_{k\in\mathbb{N}} \mathrm{Dist}_{k+1}(G)/\mathrm{Dist}_k(G)$$

[65] A similar argument can be made regarding the algebra $\mathbb{U}^{(m)}$ defined in Subsection 3.1.1, *supra*.
[66] This also holds for an affine group scheme.

is commutative.[67] Furthermore, $\mathrm{Dist}_k^+(G)$ is the same object as $\mathrm{Dist}_k(G)^+$ and $\mathrm{Dist}^+(G)$ is an ideal in $\mathrm{Dist}(G)$.

We can now use the results of Subsection 3.2.1 to obtain analogues of the universal enveloping algebras. In particular, we define the **higher universal enveloping algebra** of G of degree r to be the algebra

$$U^{[r]}(G) := U^{[p^{r+1}-1]}(\mathrm{Dist}(G)).$$

In order to gain an initial understanding of the structure of $U^{[r]}(G)$, recall that the Frobenius kernel G_s ($s \in \mathbb{N}$) is the kernel of the Frobenius homomorphism $F^s : G \to G^{(s)}$.[68] Applying the distribution functor to F^s, we get a Hopf algebra homomorphism

$$\Xi_s : \mathrm{Dist}(G) \to \mathrm{Dist}(G^{(s)}), \qquad \Xi_s(\delta)(f) = \delta(f^{p^s}).$$

Proposition 3.2.2.1. *For each $r, s \in \mathbb{N}$, the map Ξ_s induces a Hopf algebra homomorphism $\Upsilon_{r,s} : U^{[r]}(G) \to U^{[r-s]}(G^{(s)})$.*

Proof. First, note that if $f \in I_1^{k+1}$, with $f \in \mathbb{K}[G]$, then $\Xi_s(\delta)(f) = \delta(f^{p^s}) \in \delta(I_1^{p^s(k+1)})$. So if $\delta \in \mathrm{Dist}_m(G)$ for $m \in \mathbb{N}$, we have $\Xi_s(\delta) \in \mathrm{Dist}_n(G)$ for $n \geqslant \frac{m+1}{p^s} - 1$. Now, observe that $\delta(1) = 0$ implies $\Xi_s(\delta)(1) = 0$, so $\delta \in \mathrm{Dist}_m^+(G)$ for $m \in \mathbb{N}$ in fact implies that $\Xi_s(\delta) \in \mathrm{Dist}_n^+(G)$ for $n \geqslant \frac{m+1}{p^s} - 1$. We can deduce that if $\delta \in \mathrm{Dist}_m^+(G)$ for $m < p^s$ then $\Xi_s(\delta) \in \mathrm{Dist}_0^+(G) = 0$ since $\frac{m+1}{p^s} - 1 \leqslant 0$. Hence, $\Xi_s(\mathrm{Dist}_m^+(G)) = 0$ for $m < p^s$. Similarly, if $\delta \in \mathrm{Dist}_{p^{r+1}-1}^+(G)$ then $\Xi_s(\delta) \in \mathrm{Dist}_{p^{r-s+1}-1}^+(G)$.

Furthermore $\Xi_s : \mathrm{Dist}_{p^{r+1}-1}^+(G) \to \mathrm{Dist}_{p^{r-s+1}-1}^+(G) \hookrightarrow U^{[r-s]}(G)$ is an indexed algebra homomorphism. This follows because if $\delta \in \mathrm{Dist}_i^+(G)$ and $\mu \in \mathrm{Dist}_j^+(G)$ with $i + j < p^{r+1}$ then $\Xi_s(\delta) \in \mathrm{Dist}_{\lceil \frac{i+1}{p^s} \rceil - 1}^+(G)$ and $\Xi_s(\mu) \in \mathrm{Dist}_{\lceil \frac{j+1}{p^s} \rceil - 1}^+(G)$ (here $\lceil x \rceil$ denotes the smallest integer $\geqslant x$), and

$$\left\lceil \frac{i+1}{p^s} \right\rceil - 1 + \left\lceil \frac{j+1}{p^s} \right\rceil - 1 \leqslant \frac{i+j}{p^s} < p^{r-s+1},$$

and similarly for the commutator. Hence the universal property gives an algebra homomorphism $\Upsilon_{r,s} : U^{[r]}(G) \to U^{[r-s]}(G)$.

The fact that $\Upsilon_{r,s}$ is a Hopf algebra homomorphism follows from the fact that Ξ_s is a Hopf algebra homomorphism and the fact that the comultiplication, counit and antipode of $U^{[r]}(G)$ come from the corresponding maps on $\mathrm{Dist}(G)$.

□

It is straightforward to check that $U^{[r-s]}(G^{(s)}) \cong U^{[r-s]}(G)^{(s)}$, so these two notations are used interchangeably from now on.

[67]See Subsection 2.3.2, *supra*.

[68]See Subsection 2.3.4, *supra*, for details.

Lemma 3.2.2.2. *The map $\Upsilon_{r,s} : U^{[r]}(G) \to U^{[r-s]}(G^{(s)})^{[s]}$ is G-equivariant for all $r, s \in \mathbb{N}$.*

Proof. This will follow from the same fact for $\mathrm{Dist}^+_{p^{r+1}-1}(G) \to \mathrm{Dist}^+_{p^{r-s+1}-1}(G)^{[s]}$. For this to hold, it is enough that the Frobenius morphism commutes with conjugation (where in the codomain the conjugation is pre-composed with the Frobenius morphism). This condition holds since F^s is a homomorphism. □

Corollary 3.2.2.3. *The map $\Upsilon_{r,s}$ is surjective if $r \geqslant s$.*

Proof. If $x_1, \dots, x_n$ is a basis of $\mathfrak{g}$, we choose sequences of divided powers[69] such that $\Xi_s(x_i^{(p^r)}) = x_i^{(p^{r-s})}$ for $1 \leqslant i \leqslant n$. The result will follow from Lemma 3.3.1.4, *infra.* □

A special case of the previous observation is that when $r = s$ the above process gives a surjective algebra homomorphism $\Upsilon_{r,r} \colon U^{[r]}(G) \to U(\mathfrak{g})^{(r)}$, and a surjective G-module homomorphism $\Upsilon_{r,r} \colon U^{[r]}(G)^{(-r)} \to U(\mathfrak{g})^{[r]}$.

Note that if G is defined over $\mathbb{F}_p$ (e.g. if G is reductive), we may instead apply the distribution functor to the geometric Frobenius endomorphism[70] F^s_{geo}. This gives a Hopf algebra homomorphism

$$\Xi_s : \mathrm{Dist}(G) \to \mathrm{Dist}(G), \qquad \Xi_s(\delta)(f \otimes a) = \delta(f^{p^s} \otimes a).$$

In this context one can then similarly obtain, for all $r, s \in \mathbb{N}$, surjective Hopf algebra homomorphisms $\Upsilon_{r,s} : U^{[r]}(G) \to U^{[r-s]}(G)$ such that the linear maps $\Upsilon_{r,s} : U^{[r]}(G) \to U^{[r-s]}(G)^{[s]}$ are G-equivariant. When G is defined over $\mathbb{F}_p$ later in this thesis, we often prefer this interpretation of these maps.

3.3 The algebra structure of $U^{[r]}(G)$

3.3.1 Initial structural results

The key observation which allows Friedlander and Parshall to develop and study their deformation algebras is that the p-th power map gives rise to the semilinear map $\xi : \mathfrak{g} \to Z(U(\mathfrak{g}))$ defined in Subsection 2.1.3. In order to make progress with the study of the structure of $U^{[r]}(G)$ we need to construct an analogue of the map ξ. We start with the following lemma. Note that when $\delta \in \mathrm{Dist}^+_k(G)$ we already know from Subsection 2.3.2 that $\delta^p \in \mathrm{Dist}^+_{pk}(G)$.

Lemma 3.3.1.1. *If $\delta \in \mathrm{Dist}^+_k(G)$, then $\delta^p \in \mathrm{Dist}^+_{pk-1}(G)$.*

Proof. Recall that $\mathbb{K}[G] = \mathbb{K} \oplus I_1$. Hence, for $m \in \mathbb{N}$, we have that $\mathbb{K}[G]^{\otimes m} = \sum_{P_i \in \{\mathbb{K}, I_1\}} P_1 \otimes P_2 \otimes \cdots \otimes P_m$. Using this and the counitary property of the Hopf

[69] See Subsection 2.4.2.
[70] See Subsection 2.3.4 for the definition.

algebra structure of $\mathbb{K}[G]$, we have for $f \in I_1$,

$$\Delta_{m-1}(f) \in f \otimes 1 \otimes \cdots \otimes 1 + 1 \otimes f \otimes \cdots \otimes 1 + \cdots + 1 \otimes 1 \otimes \cdots \otimes f + \sum_{\substack{a_i \in \{0,1\} \\ 2 \leqslant \sum a_i \leqslant m}} I_1^{a_1} \otimes \cdots \otimes I_1^{a_m},$$

where Δ_{m-1} is defined inductively by setting Δ_1 as the comultiplication of $\mathbb{K}[G]$ and $\Delta_l := (\Delta_{l-1} \otimes \mathrm{Id}) \circ \Delta$ for $l > 1$. One can hence show by induction that for $f_1, \ldots, f_n \in I_1$, with $n \in \mathbb{N}$, we have

$$\Delta_{m-1}(f_1 \ldots f_n) \in \prod_{i=1}^{n} (f_i \otimes 1 \otimes \cdots \otimes 1 + 1 \otimes f_i \otimes \cdots \otimes 1 + \cdots + 1 \otimes 1 \otimes \cdots \otimes f_i) + \sum_{\substack{0 \leqslant a_i \leqslant n \\ n+1 \leqslant \sum a_i \leqslant mn}} I_1^{a_1} \otimes \cdots \otimes I_1^{a_m}.$$

Rewriting this slightly, we get

$$\Delta_{m-1}(f_1 \ldots f_n) \in \prod_{i=1}^{n} (f_i \otimes 1 \otimes \cdots \otimes 1 + 1 \otimes f_i \otimes \cdots \otimes 1 + \cdots + 1 \otimes 1 \otimes \cdots \otimes f_i) + \sum_{j=1}^{m} \sum_{\substack{0 \leqslant a_i \leqslant n \\ n+1 \leqslant \sum a_i \leqslant mn \\ a_j = 0}} I_1^{a_1} \otimes \cdots \otimes I_1^{a_m} + \sum_{\substack{1 \leqslant a_i \leqslant n \\ \sum a_i = n+1}} I_1^{a_1} \otimes \cdots \otimes I_1^{a_m}.$$

We now fix $m = p$ and $n = pk$. Given $\delta \in \mathrm{Dist}_k^+(G)$ (so $\delta(I_1^{k+1}) = 0$ and $\delta(1) = 0$) and $f_1, \ldots, f_{pk} \in I_1$ we have that

$$\delta^p(f_1 \ldots f_{pk}) = (\delta \otimes \delta \otimes \cdots \otimes \delta)(\Delta_{p-1}(f_1 \ldots f_{pk})) \in (\delta \otimes \delta \otimes \cdots \otimes \delta) \left(\prod_{i=1}^{pk} (f_i \otimes 1 \otimes \cdots \otimes 1 + 1 \otimes f_i \otimes \cdots \otimes 1 + \cdots + 1 \otimes 1 \otimes \cdots \otimes f_i) \right) + \sum_{j=1}^{p} \sum_{\substack{0 \leqslant a_i \leqslant pk \\ pk+1 \leqslant \sum a_i \leqslant p^2 k \\ a_j = 0}} \delta(I_1^{a_1}) \ldots \delta(I_1^{a_m}) + \sum_{\substack{1 \leqslant a_i \leqslant pk \\ pk+1 = \sum a_i}} \delta(I_1^{a_1}) \ldots \delta(I_1^{a_p}).$$

Since $\delta(1) = 0$, we get

$$\sum_{j=1}^{p} \sum_{\substack{0 \leqslant a_i \leqslant pk \\ pk+1 \leqslant \sum a_i \leqslant p^2 k \\ a_j = 0}} \delta(I_1^{a_1}) \ldots \delta(I_1^{a_m}) = 0.$$

Since $a_1 + \cdots + a_p = pk + 1$ implies $a_i \geqslant k + 1$ for some i, and $\delta(I_1^{k+1}) = 0$, we also have

$$\sum_{\substack{1 \leqslant a_i \leqslant pk \\ pk+1 = \sum a_i}} \delta(I_1^{a_1}) \dots \delta(I_1^{a_p}) = 0.$$

Now, we want to compute $(\delta \otimes \delta \otimes \cdots \otimes \delta)(\prod_{i=1}^{pk}(f_i \otimes 1 \otimes \cdots \otimes 1 + 1 \otimes f_i \otimes \cdots \otimes 1 + \cdots + 1 \otimes 1 \otimes \cdots \otimes f_i))$.

Observe that

$$\prod_{i=1}^{pk}(f_i \otimes 1 \otimes \cdots \otimes 1 + 1 \otimes f_i \otimes \cdots \otimes 1 + \cdots + 1 \otimes 1 \otimes \cdots \otimes f_i) = \sum f_{A_1} \otimes \cdots \otimes f_{A_p},$$

where the sum is over all ordered partitions[71] $A_1, \dots, A_p$ of the set $\{1, \dots, pk\}$ where the sets can be empty, and where, if $A_i = \{j_1, \dots, j_s\}$ with $j_1 < \dots < j_s$, we denote $f_{A_i} = f_{j_1} f_{j_2} \dots f_{j_s}$. Then

$$\begin{aligned}(\delta \otimes \delta \otimes \cdots \otimes \delta) \left(\prod_{i=1}^{pk}(f_i \otimes 1 \otimes \cdots \otimes 1 + 1 \otimes f_i \otimes \cdots \otimes 1 + \cdots + 1 \otimes 1 \otimes \cdots \otimes f_i) \right) \\ = \sum \delta(f_{A_1}) \dots \delta(f_{A_p})\end{aligned}$$

where the sum is over the same set as before.

For ordered partitions containing empty sets, $\delta(f_{A_i}) = \delta(1) = 0$ for those i with $A_i = \varnothing$. Furthermore, if two ordered partitions containing no empty sets are rearrangements of each other, they give the same summand in the above sum since $\mathbb{K}$ is a field. In particular, there are $p!$ such partitions which give the same summand, so this summand appears $p!$ times. Hence

$$\begin{aligned}(\delta \otimes \delta \otimes \cdots \otimes \delta) \left(\prod_{i=1}^{pk}(f_i \otimes 1 \otimes \cdots \otimes 1 + 1 \otimes f_i \otimes \cdots \otimes 1 + \cdots + 1 \otimes 1 \otimes \cdots \otimes f_i) \right) \\ = \sum p! \delta(f_{A_1}) \dots \delta(f_{A_p}) = 0\end{aligned}$$

where this time the second sum is over *unordered partitions* with p non-empty sets in them.

Hence, we have that $\delta^p(f_1 \dots f_{pk}) = 0$. That is to say, $\delta^p \in \mathrm{Dist}^+_{pk-1}(G)$. □

In particular, if $\delta \in \mathrm{Dist}^+_{p^r}(G)$ then $\delta^p \in \mathrm{Dist}^+_{p^{r+1}-1}(G)$. This allows us to define a map $\xi_r : \mathrm{Dist}^+_{p^r}(G) \to U^{[r]}(G)$ as $\xi_r(\delta) = \delta^{\otimes p} - \delta^p$ where the first exponent is in $U^{[r]}(G)$ and the second is in $\mathrm{Dist}(G)$.

Lemma 3.3.1.2. *The map ξ_r is semilinear.*

Proof. Clearly $\xi_r(\lambda\delta) = \lambda^p \xi_r(\delta)$ if $\lambda \in \mathbb{K}$ and $\delta \in \mathrm{Dist}^+_{p^r}(G)$. We now want to show

[71] Ordered partition means for example that $\{1, 2\}, \{3, 4\}$ is different from $\{3, 4\}, \{1, 2\}$.

$\xi_r(\mu + \rho) = \xi_r(\mu) + \xi_r(\rho)$ for $\mu, \rho \in \mathrm{Dist}^+_{p^r}(G)$. Observe that, by definition,

$$\xi_r(\mu + \rho) = (\mu + \rho)^{\otimes p} - (\mu + \rho)^p.$$

We have that

$$(\mu + \rho)^{\otimes p} = \sum_{a_i \in \{0,1\}} \eta_{a_1} \otimes \cdots \otimes \eta_{a_p},$$

where $\eta_0 = \mu$ and $\eta_1 = \rho$. Applying $\mu \otimes \rho - \rho \otimes \mu = [\mu, \rho] \in \mathrm{Dist}^+_{2p^r-1}(G)$, we get

$$(\mu + \rho)^{\otimes p} = \sum_{i=0}^{p} \binom{p}{i} \mu^{\otimes i} \otimes \rho^{\otimes (p-i)} - \Psi$$

where Ψ is a sum of terms in $U^{[r]}(G)$, each of which is the tensor product of elements of $\mathrm{Dist}(G)$ where the sum of the grades is less than p^{r+1}. Hence, Ψ is obtained from the product of these elements in $\mathrm{Dist}(G)$, by the definition of $U^{[r]}(G)$. Since p is the characteristic of $\mathbb{K}$, we get

$$(\mu + \rho)^{\otimes p} = \mu^{\otimes p} + \rho^{\otimes p} - \Psi.$$

Similarly,

$$(\mu + \rho)^p = \sum_{a_i \in \{0,1\}} \eta_{a_1} \dots \eta_{a_p},$$

where $\eta_0 = \mu$ and $\eta_1 = \rho$. Applying $\mu\rho - \rho\mu = [\mu, \rho] \in \mathrm{Dist}_{2p^r-1}(G)$, we get

$$(\mu + \rho)^p = \sum_{i=0}^{p} \binom{p}{i} \mu^i \rho^{p-i} - \Psi$$

where Ψ is exactly the same Ψ as above since the multiplication in the expression of Ψ is the same in $\mathrm{Dist}(G)$ and $U^{[r]}(G)$. So

$$(\mu + \rho)^p = \mu^p + \rho^p - \Psi.$$

Hence $\xi_r(\mu + \rho) = \xi_r(\mu) + \xi_r(\rho)$ □

For $k \leqslant r$, define X_{p^k} to be the $\mathbb{K}$-span in $U^{[r]}(G)$ of

$$\{\mu \in \mathrm{Dist}^+_{p^k}(G) \mid \mu = \rho_1\rho_2 \,\text{for}\, \rho_i \in \mathrm{Dist}_{j_i}(G) \,\text{with}\, j_1 + j_2 \leqslant p^k,\ j_1, j_2 < p^k\}.$$

Define Y_{p^k} to be a vector space complement of this subspace in $\mathrm{Dist}^+_{p^k}(G)$; when G is reductive, we take it to be the one with basis $\{\mathbf{e}_\alpha^{(p^k)}, \binom{\mathbf{h}_t}{p^k} \mid \alpha \in \Phi, 1 \leqslant t \leqslant d\}$ (see Subsection 2.4.2 for the notation). The next proposition shows that ξ_r is only non-trivial outside of the subspace X_{p^r}.

Proposition 3.3.1.3. *For all $0 \leqslant k \leqslant r$, we have $\xi_r(X_{p^k}) = 0$.*

Proof. Since $X_{p^k} \subseteq X_{p^r}$ for all $0 \leqslant k \leqslant r$, it is sufficient to prove that $\xi_r(X_{p^r}) = 0$.

Suppose $\mu \in \mathrm{Dist}_i(G)$, $\rho \in \mathrm{Dist}_j(G)$, where $i+j \leqslant p^r$ and $i,j > 0$. So $\mu\rho \in \mathrm{Dist}_{p^r}(G)$. Consider $\xi_r(\mu\rho) = (\mu\rho)^{\otimes p} - (\mu\rho)^p$. Note that $\mu\rho - \mu \otimes \rho = 0$ as $i+j \leqslant p^r < p^{r+1}$. We have

$$(\mu\rho)^{\otimes p} = \mu \otimes (\rho \otimes \mu) \otimes \cdots \otimes (\rho \otimes \mu) \otimes \rho.$$

Furthermore $\rho \otimes \mu - \mu \otimes \rho = [\rho, \mu] \in \mathrm{Dist}_{p^r-1}(G)$. Hence

$$(\mu\rho)^{\otimes p} = \mu^{\otimes p} \otimes \rho^{\otimes p} - \Phi,$$

where Φ is a sum of terms in $U^{[r]}(G)$, each of which is the tensor product of elements of $\mathrm{Dist}(G)$ where the sum of the grades is less than p^{r+1}. Hence, Φ is obtained from the product of these elements in $\mathrm{Dist}(G)$. Similarly, we have

$$(\mu\rho)^p = \mu(\rho\mu)\dots(\rho\mu)\rho.$$

Since $\rho\mu - \mu\rho = [\rho, \mu]$ by definition, we get that

$$(\mu\rho)^p = \mu^p\rho^p - \Phi,$$

where Φ is exactly the same as above, since it doesn't matter when calculating Φ if the multiplication is done in $\mathrm{Dist}(G)$ or in $U^{[r]}(G)$ because of the grades of the elements being multiplied.

Hence, $\xi_r(\mu\rho) = (\mu\rho)^{\otimes p} - (\mu\rho)^p = \mu^{\otimes p} \otimes \rho^{\otimes p} - \mu^p\rho^p$. Since $\mu \in \mathrm{Dist}_i(G)$ and $i < p^r$, we have $\mu^{\otimes p} = \mu^p$, and similarly for ρ. So $\xi_r(\mu\rho) = \mu^p \otimes \rho^p - \mu^p\rho^p$. Furthermore, $\mu^p \in \mathrm{Dist}_{pi-1}(G)$ and $\rho^p \in \mathrm{Dist}_{pj-1}(G)$, so $\mu^p \otimes \rho^p = \mu^p\rho^p$, so $\xi_r(\mu\rho) = 0$. □

We would like to show that the image of ξ_r is central in $U^{[r]}(G)$. To achieve this, we start by constructing a basis of the higher universal enveloping algebra, analogous to the Poincaré-Birkhoff-Witt basis for $U(\mathfrak{g})$ demonstrated in Theorem 2.1.1.2.

From Proposition 2.3.4.1 there is an inclusion of vector spaces $\mathrm{Dist}^+_{p^r-1}(G) \hookrightarrow \mathrm{Dist}(G_r) \subseteq \mathrm{Dist}(G)$ which clearly satisfies the necessary conditions to employ the universal property of $U^{[r-1]}(G)$ and obtain an algebra homomorphism

$$\pi_{r-1} : U^{[r-1]}(G) \to \mathrm{Dist}(G_r).$$

If we pick a basis $x_1, \dots, x_n$ of $\mathfrak{g}$, then we saw in Subsection 2.4.2 that $\mathrm{Dist}(G_r)$ has a divided power basis

$$\{x_1^{(a_1)}x_2^{(a_2)}\dots x_n^{(a_n)} \mid 0 \leqslant a_i < p^r \text{ for all } 1 \leqslant i \leqslant n\}.$$

We may then easily to deduce that π_{r-1} is surjective.

Furthermore, it is straightforward to see that for $\delta \in \mathrm{Dist}^+_{p^r-1}(G)$ the equality

$\pi_{r-1}(\delta)^p = \pi_{r-1}(\delta^p)$ holds. Hence, letting R_{r-1} be the ideal of $U^{[r-1]}(G)$ generated by $\delta^{\otimes p} - \delta^p$ for $\delta \in \mathrm{Dist}^+_{p^{r-1}}(G)$, there is a surjective algebra homomorphism

$$\overline{\pi_{r-1}} : U^{[r-1]}(G)/R_{r-1} \twoheadrightarrow \mathrm{Dist}(G_r).$$

Lemma 3.3.1.4. *The algebra $U^{[r-1]}(G)$ is spanned by the set*

$$\left\{ \begin{array}{c} x_1^{(a_1)} \otimes (x_1^{(p^{r-1})})^{\otimes b_1} \otimes x_2^{(a_2)} \otimes (x_2^{(p^{r-1})})^{\otimes b_2} \otimes \cdots \otimes x_n^{(a_n)} \otimes (x_n^{(p^{r-1})})^{\otimes b_n} \\ \textit{such that } 0 \leqslant a_i < p^{r-1},\ b_i \geqslant 0,\ 1 \leqslant i \leqslant n \end{array} \right\}.$$

Proof. It is obvious from the basis of $\mathrm{Dist}_{p^r-1}(G)$ given in Subsection 2.4.2 that these elements generate $U^{[r-1]}(G)$. Hence, using a filtration argument, all that remains is to make the following observations:

(i) For $1 \leqslant i \leqslant n$, if $0 \leqslant s,t \leqslant p^{r-1}$, then $x_i^{(s)} \otimes x_i^{(t)} - \binom{s+t}{s} x_i^{(s+t)}$ lies in the $\mathbb{K}$-span of the set

$$\left\{ \begin{array}{c} x_1^{(a_1)} \otimes x_2^{(a_2)} \otimes \cdots \otimes x_n^{(a_n)} \\ \text{with } 0 \leqslant a_j < p^{r-1},\ 1 \leqslant j \leqslant n, \text{ and } \sum_{j=1}^n a_j < s+t \end{array} \right\}.$$

Note here that $\binom{s+t}{s} = 0$ if $s+t \geqslant p^{r-1}$ and $s,t < p^{r-1}$.

(ii) For $0 \leqslant s,t \leqslant p^{r-1}$ and $1 \leqslant i \leqslant j \leqslant n$, the commutator $x_j^{(t)} \otimes x_i^{(s)} - x_i^{(s)} \otimes x_j^{(t)}$ lies in the $\mathbb{K}$-span of the set

$$\left\{ \begin{array}{c} x_1^{(a_1)} \otimes (x_1^{(p^{r-1})})^{\otimes b_1} \otimes x_2^{(a_2)} \otimes (x_2^{(p^{r-1})})^{\otimes b_2} \otimes \cdots \otimes x_n^{(a_n)} \otimes (x_n^{(p^{r-1})})^{\otimes b_n} \\ \text{with } 0 \leqslant a_k < p^{r-1},\ b_k \geqslant 0,\ 1 \leqslant k \leqslant n, \text{ and} \sum_{k=1}^n (a_k + b_k p^{r-1}) < s+t \end{array} \right\}.$$

These observations all follow from the defining relations of $U^{[r-1]}(G)$ and calculations with the divided power basis of $\mathrm{Dist}(G_r) = \mathbb{K}[G_r]^*$. □

Corollary 3.3.1.5. *The algebra $U^{[r-1]}(G)/R_{r-1}$ is spanned by the set*

$$\left\{ \begin{array}{c} x_1^{(a_1)} \otimes (x_1^{(p^{r-1})})^{\otimes b_1} \otimes x_2^{(a_2)} \otimes (x_2^{(p^{r-1})})^{\otimes b_2} \otimes \cdots \otimes x_n^{(a_n)} \otimes (x_n^{(p^{r-1})})^{\otimes b_n} \\ \textit{such that } 0 \leqslant a_i < p^{r-1},\ 0 \leqslant b_i < p,\ 1 \leqslant i \leqslant n \end{array} \right\}.$$

Proof. This follows from the above lemma since $\delta \in \mathrm{Dist}_{p^{r-1}}(G)$ implies $\delta^p \in \mathrm{Dist}_{p^r-1}(G)$ by Lemma 3.3.1.1. □

Hence, $\dim(U^{[r-1]}(G)/R_{r-1}) \leqslant p^{r\dim(\mathfrak{g})}$. However, $U^{[r-1]}(G)/R_{r-1}$ surjects onto $\mathrm{Dist}(G_r)$, which, by Proposition 2.3.4.1, has dimension $p^{r\dim(\mathfrak{g})}$. Thus, we find that $U^{[r-1]}(G)/R_{r-1} \cong \mathrm{Dist}(G_r)$.

In particular, the universal property of the algebra $U^{[r-1]}(G)/R_{r-1}$ gives an algebra homomorphism $\mathrm{Dist}(G_r) \to U^{[r]}(G)$. Composing with π_r then gives an algebra homomorphism $\mathrm{Dist}(G_r) \to \mathrm{Dist}(G_{r+1})$ which, by considering the effect on the basis, is clearly injective. Hence, there is an inclusion $\mathrm{Dist}(G_r) \hookrightarrow U^{[r]}(G)$ of algebras.

The above results show that $\mathrm{Dist}(G_r)$ is a Hopf subalgebra of $U^{[r]}(G)$, since the coalgebra structure on $U^{[r]}(G)$ is extended from the coalgebra structure on $\mathrm{Dist}_{p^{r+1}-1}(G) \subseteq \mathrm{Dist}(G_r)$ using the universal property given in Proposition 3.2.1.1, and similarly for the antipode. We can say even more about the structure of this Hopf subalgebra.

Lemma 3.3.1.6. *For an algebraic group G, the algebra $U^{[r]}(G)$ satisfies the following properties:*

(1) $\mathrm{Dist}(G_r)$ *is a normal Hopf subalgebra of* $U^{[r]}(G)$*.*

(2) $U^{[r]}(G)$ *is free as a left and right* $\mathrm{Dist}(G_r)$*-module.*

(3) $U^{[r]}(G)$ *is faithfully flat as a left and right* $\mathrm{Dist}(G_r)$*-module.*

(4) $U^{[r]}(G)/\mathrm{Dist}^+(G_r)U^{[r]}(G)$ *is isomorphic to the Hopf algebra* $U(\mathfrak{g})$*.*

(5) $\mathrm{Dist}(G_r) \subseteq U^{[r]}(G)$ *is a* $U(\mathfrak{g})$*-Galois extension, with* $\mathrm{Dist}(G_r) = U^{[r]}(G)^{coU(\mathfrak{g})}$.

Proof. Since $U^{[r]}(G)$ is cocommutative, to show normality of of $\mathrm{Dist}(G_r)$ in $U^{[r]}(G)$ it is enough enough to prove closure under the left adjoint. Since

$$\mathrm{ad}_l(aa')(b) = \mathrm{ad}_l(a)\mathrm{ad}_l(a')(b)$$

and

$$\mathrm{ad}_l(a)(bb') = \sum (\mathrm{ad}_l(a_{(1)})b)(\mathrm{ad}_l(a_{(2)})b')$$

for $a, a' \in A$ and $b, b' \in B$, it is enough to show closure for generators of A and B. We saw in Proposition 2.3.4.1 that $\mathrm{Dist}(G_r) \subseteq \mathrm{Dist}(G)$ is generated by $\mathrm{Dist}_{p^r-1}(G)$, and $U^{[r]}(G)$ is generated by $\mathrm{Dist}_{p^r}(G)$. Let $\delta \in \mathrm{Dist}_{p^r}(G)$ and $\mu \in \mathrm{Dist}_{p^r-1}(G)$. Then

$$\mathrm{ad}_l(\delta)(\mu) = \sum \delta_{(1)} \otimes \mu \otimes S(\delta_{(2)}),$$

where the $\otimes$ represents the multiplication in $U^{[r]}(G)$, and we have $\delta_{(1)} \in \mathrm{Dist}_i(G)$, $\delta_{(2)} \in \mathrm{Dist}_j(G)$ with $i + j = p^r$. In particular, $i + p^r - 1 + j < p^{r+1}$ and so in fact

$$\mathrm{ad}_l(\delta)(\mu) = \sum \delta_{(1)}\mu S(\delta_{(2)}),$$

with the multiplication now in $\mathrm{Dist}_{p^{r+1}-1}(G)$, the restriction of the multiplication in $\mathrm{Dist}(G)$. Since $\mathrm{Dist}(G_r)$ is normal in $\mathrm{Dist}(G)$,[72] we hence conclude that $\mathrm{ad}_l(\delta)(\mu) \in \mathrm{Dist}(G_r)$. This proves (1).

Part (2) then follows from Theorem 2.1(2) in [Schneider, 1993], and (3) follows from (2). Furthermore, (4) is easy to see from the results of Subsection 3.2.2 and Lemma 3.3.1.4, and (5) follows from Remark 1.1(4) in [Schneider, 1990]. □

This lemma allows us to understand the structure of $U^{[r]}(G)$ as a Hopf algebra.

[72] See I.7.18 in [Jantzen, 1987].

Proposition 3.3.1.7. *The $U(\mathfrak{g})^{(r)}$-extension* $\mathrm{Dist}(G_r) \subseteq U^{[r]}(G)$ *is $U(\mathfrak{g})^{(r)}$-cleft.*

Proof. We need to show that there is a convolution-invertible right $U(\mathfrak{g})^{(r)}$-comodule map $\gamma : U(\mathfrak{g})^{(r)} \to U^{[r]}(G)$. Since $U(\mathfrak{g})^{(r)}$ has basis

$$\{x_1^{a_1} x_2^{a_2} \dots x_n^{a_n} \mid a_i \geqslant 0,\ 1 \leqslant i \leqslant n\},$$

we simply need to define $\gamma(x_1^{a_1} x_2^{a_2} \dots x_n^{a_n})$ for all $a_1, a_2, \dots, a_n \geqslant 0$.

As such, we define

$$\gamma(x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}) = (x_1^{(p^r)})^{\otimes a_1} \otimes (x_2^{(p^r)})^{\otimes a_2} \otimes \cdots \otimes (x_n^{(p^r)})^{\otimes a_n} \in U^{[r]}(G)$$

for all $a_1, a_2, \dots, a_n \geqslant 0$.

To show that γ is a $U(\mathfrak{g})^{(r)}$-comodule map we need to show that, for $y \in U(\mathfrak{g})^{(r)}$,

$$\sum \gamma(y)_{(1)} \otimes \overline{\gamma(y)_{(2)}} = \sum \gamma(y_{(1)}) \otimes y_{(2)}$$

where we use Sweedler's Σ-notation and we write $\overline{\gamma(y)_{(2)}}$ for $\Upsilon_{r,r}(\gamma(y)_{(2)})$.

It is enough to show this for basis elements. Note that, if $y = x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}$ with $a_1, a_2, \dots, a_n \geqslant 0$, then

$$\begin{aligned}\Delta(y) &= (x_1 \otimes 1 + 1 \otimes x_1)^{a_1} (x_2 \otimes 1 + 1 \otimes x_2)^{a_2} \dots (x_n \otimes 1 + 1 \otimes x_n)^{a_n} \\ &= \sum_{b_i + c_i = a_i} \binom{a_1}{b_1} \binom{a_2}{b_2} \cdots \binom{a_n}{b_n} x_1^{b_1} x_2^{b_2} \dots x_n^{b_n} \otimes x_1^{c_1} x_2^{c_2} \dots x_n^{c_n}.\end{aligned}$$

Furthermore, writing $\Delta_{U(\mathfrak{g})^{(r)}}$ for the $U(\mathfrak{g})^{(r)}$-comodule map of the comodule $U^{[r]}(G)$,

$$\begin{aligned}&\Delta_{U(\mathfrak{g})^{(r)}}((x_1^{(p^r)})^{\otimes a_1} \otimes (x_2^{(p^r)})^{\otimes a_2} \otimes \cdots \otimes (x_n^{(p^r)})^{\otimes a_n}) \\ &\qquad = \Delta_{U(\mathfrak{g})^{(r)}}(x_1^{(p^r)})^{\otimes a_1} \otimes \Delta_{U(\mathfrak{g})^{(r)}}(x_2^{(p^r)})^{\otimes a_2} \otimes \cdots \otimes \Delta_{U(\mathfrak{g})^{(r)}}(x_n^{(p^r)})^{\otimes a_n},\end{aligned}$$

while, for any $1 \leqslant i \leqslant n$,

$$\Delta_{U(\mathfrak{g})^{(r)}}(x_i^{(p^r)}) = \sum_{j=0}^{p^r} x_i^{(j)} \otimes \overline{x_i^{(p^r - j)}} = x_i^{(p^r)} \otimes 1 + 1 \otimes x_i$$

since $\overline{x_i^{(s)}} = 0$ for all $0 < s < p^r$.

Hence, $\sum \gamma(y)_{(1)} \otimes \overline{\gamma(y)_{(2)}}$ equals

$$\sum_{b_i + c_i = a_i} \binom{a_1}{b_1} \binom{a_2}{b_2} \cdots \binom{a_n}{b_n} ((x_1^{(p^r)})^{\otimes b_1} \otimes (x_2^{(p^r)})^{\otimes b_2} \otimes \cdots \otimes (x_n^{(p^r)})^{\otimes b_n}) \otimes (x_1^{c_1} x_2^{c_2} \dots x_n^{c_n})$$

and $\sum \gamma(y_{(1)}) \otimes y_{(2)}$ equals

$$\sum_{b_i+c_i=a_i} \binom{a_1}{b_1}\binom{a_2}{b_2}\cdots\binom{a_n}{b_n}((x_1^{(p^r)})^{\otimes b_1}\otimes(x_2^{(p^r)})^{\otimes b_2}\otimes\cdots\otimes(x_n^{(p^r)})^{\otimes b_n})\otimes(x_1^{c_1}x_2^{c_2}\ldots x_n^{c_n}).$$

Thus, γ is a $U(\mathfrak{g})^{(r)}$-comodule map. Furthermore, γ is convolution-invertible (with convolution inverse $S\gamma$), since $U^{[r]}(G)$ is a Hopf algebra. □

By Theorem 2.2.2.4, $\mathrm{Dist}(G_r) \subseteq U^{[r]}(G)$ has the normal basis property. Hence, $U^{[r]}(G) \cong \mathrm{Dist}(G_r) \otimes U(\mathfrak{g})^{(r)}$ as left $\mathrm{Dist}(G_r)$-modules and right $U(\mathfrak{g})^{(r)}$-comodules. Furthermore, the same theorem shows that

$$U^{[r]}(G) \cong \mathrm{Dist}(G_r)\#_\sigma U(\mathfrak{g})^{(r)},$$

a crossed product of $\mathrm{Dist}(G_r)$ with $U(\mathfrak{g})^{(r)}$.[73]

Corollary 3.3.1.8. *The $\mathbb{K}$-algebra $U^{[r]}(G)$ has basis*

$$\{x_1^{(a_1)}x_2^{(a_2)}\ldots x_n^{(a_n)}(x_1^{(p^r)})^{b_1}(x_2^{(p^r)})^{b_2}\ldots(x_n^{(p^r)})^{b_n} \mid 0 \leqslant a_i < p^r,\, 0 \leqslant b_i,\, 1 \leqslant i \leqslant n\}.$$

3.3.2 Reductive groups

For this section, unless specified otherwise, G will be a reductive algebraic group over an algebraically closed field $\mathbb{K}$ of characteristic $p > 0$. We keep the notation from Subsection 2.4.1; for example, B is a Borel subgroup of G containing a maximal torus T and with corresponding root system Φ. We show that when G is a reductive group we may view the higher universal enveloping algebra of G as coming from a $\mathbb{Z}_{(p)}$-form of the universal enveloping algebra of $\mathfrak{g}$. Recall here that $\mathbb{Z}_{(p)} := \{\frac{a}{b} \in \mathbb{Q} \mid \mathrm{hcf}(a,b) = 1,\, p \nmid b\}$ is a commutative local ring.

As discussed in Subsection 2.4.2, throughout this thesis we abuse notation by using the same symbols $\mathbf{e}_\alpha$ and $\mathbf{h}_t$ for the corresponding elements of a Chevalley basis over any base ring. One may see this abuse, for example, in the following statement: the elements $\mathbf{e}_\alpha \in \mathfrak{g}_\mathbb{C}$ for $\alpha \in \Phi$ form a Chevalley system in $\mathfrak{g}_\mathbb{C}$, where a Chevalley system is as defined in [Bourbaki, 1975, ch. VIII, §12]. Here, $\mathfrak{g}_\mathbb{C}$ is the complex reductive Lie algebra corresponding to $\mathfrak{g}$ over the field $\mathbb{C}$.

Let us recall a useful construction of the standard bases for the universal enveloping algebra $U(\mathfrak{g})$ and the distribution algebra $\mathrm{Dist}(G)$. In both cases we start by considering the complex reductive Lie algebra $\mathfrak{g}_\mathbb{C}$, and we look at elements in the universal enveloping algebra $U(\mathfrak{g}_\mathbb{C})$. Recall from the Poincaré-Birkhoff-Witt

[73] Here, $\sigma : U(\mathfrak{g})^{(r)} \otimes U(\mathfrak{g})^{(r)} \to \mathrm{Dist}(G_r)$ is a cocycle as defined in Subsection 2.2.2, where the reader can also find the definition of a crossed product. The precise description of σ can be found in Proposition 7.2.3 in [Montgomery, 1993].

theorem that $U(\mathfrak{g}_{\mathbb{C}})$ has $\mathbb{C}$-basis

$$\left\{ \prod_{\alpha\in\Phi^+} \mathbf{e}_\alpha^{i_\alpha} \prod_{t=1}^{d} \mathbf{h}_t^{k_t} \prod_{\alpha\in\Phi^+} \mathbf{e}_{-\alpha}^{j_\alpha} \;\middle|\; 0 \leqslant i_\alpha, j_\alpha, k_t \right\}.$$

We then look at the following $\mathbb{Z}$-forms in $U(\mathfrak{g}_{\mathbb{C}})$:

$$U(\mathfrak{g})_{\mathbb{Z}} = \mathbb{Z}\left\{ \prod_{\alpha\in\Phi^+} \mathbf{e}_\alpha^{i_\alpha} \prod_{t=1}^{d} \mathbf{h}_t^{k_t} \prod_{\alpha\in\Phi^+} \mathbf{e}_{-\alpha}^{j_\alpha} \;\middle|\; 0 \leqslant i_\alpha, j_\alpha, k_t \right\},$$

$$\widetilde{U}(\mathfrak{g})_{\mathbb{Z}} = \mathbb{Z}\left\{ \prod_{\alpha\in\Phi^+} \mathbf{e}_\alpha^{(i_\alpha)} \prod_{t=1}^{d} \binom{\mathbf{h}_t}{k_t} \prod_{\alpha\in\Phi^+} \mathbf{e}_{-\alpha}^{(j_\alpha)} \;\middle|\; 0 \leqslant i_\alpha, j_\alpha, k_t \right\}$$

where $\mathbf{e}_\alpha^{(i_\alpha)} := \frac{\mathbf{e}_\alpha^{i_\alpha}}{i_\alpha!}$ and $\binom{\mathbf{h}_t}{k_t} := \frac{\mathbf{h}_t(\mathbf{h}_t-1)\dots(\mathbf{h}_t-k_t+1)}{k_t!}$ as in Subsection 2.4.2. Recall that we call $\mathbf{e}_\alpha^{(i_\alpha)}$ and $\binom{\mathbf{h}_t}{k_t}$ **divided powers** of $\mathbf{e}_\alpha$ and $\mathbf{h}_t$.

It is easy to see that the first of these is a $\mathbb{Z}$-form from the definitions of the commutators, while the fact that the second is a $\mathbb{Z}$-form is proved in [Kostant, 1966] in the case when G is semisimple and simply-connected – the more general result can be found in [Jantzen, 1987, II.1.12]. From this, we get $U(\mathfrak{g}) = U(\mathfrak{g})_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{K}$ and $\mathrm{Dist}(G) = \widetilde{U}(\mathfrak{g})_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{K}$. To obtain a similar basis for the algebra $U^{[r]}(G)$ we apply the same process with a $\mathbb{Z}_{(p)}$-form.[74]

Given an integer $M = a_0 + a_1 p + \dots + a_r p^r$ where $0 \leqslant a_0, \dots, a_{r-1} < p$ and $a_r \geqslant 0$, we define

$$\mathbf{e}_\alpha^{[\![M]\!]} := \mathbf{e}_\alpha^{a_0} (\mathbf{e}_\alpha^{(p)})^{a_1} \dots (\mathbf{e}_\alpha^{(p^r)})^{a_r} \in U(\mathfrak{g}_{\mathbb{C}})$$

for $\alpha \in \Phi$. Furthermore, define

$$\binom{\mathbf{h}_t}{[\![M]\!]} := \binom{\mathbf{h}_t}{1}^{a_0} \binom{\mathbf{h}_t}{p}^{a_1} \dots \binom{\mathbf{h}_t}{p^r}^{a_r} \in U(\mathfrak{g}_{\mathbb{C}})$$

for $1 \leqslant t \leqslant d$.

Proposition 3.3.2.1. *The subset*

$$U^{[\![r]\!]}(\mathfrak{g})_{\mathbb{Z}_{(p)}} := \mathbb{Z}_{(p)}\left\{ \prod_{\alpha\in\Phi^+} \mathbf{e}_\alpha^{[\![i_\alpha]\!]} \prod_{t=1}^{d} \binom{\mathbf{h}_t}{[\![k_t]\!]} \prod_{\alpha\in\Phi^+} \mathbf{e}_{-\alpha}^{[\![j_\alpha]\!]} \;\middle|\; 0 \leqslant i_\alpha, j_\alpha, k_t \right\} \subseteq U(\mathfrak{g}_{\mathbb{C}})$$

is a well-defined $\mathbb{Z}_{(p)}$-form of $U(\mathfrak{g}_{\mathbb{C}})$.

Proof. For this to be well defined, we need to show that it is closed under multiplication. It is clearly enough to show that certain commutators lie inside $U^{[\![r]\!]}(\mathfrak{g})_{\mathbb{Z}_{(p)}}$.

[74] Corollary 3.3.1.8 already gives us a basis of $U^{[r]}(G)$. However, for later results - in particular, showing that the image of ξ_r is central in $U^{[r]}(G)$ - it is useful to have more familiarity with this basis in the reductive case. For this reason, we give here a different construction of a Poincaré-Birkhoff-Witt basis for higher universal enveloping algebras of reductive groups.

Let us introduce the notation

$$\widetilde{U}^{[\![r]\!]}(\mathfrak{g})_{\mathbb{Z}_{(p)}} := \mathbb{Z}_{(p)} \left\{ \prod_{\alpha\in\Phi^+} \mathbf{e}_\alpha^{(i_\alpha)} \prod_{t=1}^{d} \binom{\mathbf{h}_t}{k_t} \prod_{\alpha\in\Phi^+} \mathbf{e}_{-\alpha}^{(j_\alpha)} \;\middle|\; 0 \leqslant i_\alpha, j_\alpha, k_t < p^{r+1} \right\},$$

which lies inside $\widetilde{U}(\mathfrak{g})_{\mathbb{Z}_{(p)}} \cap U^{[\![r]\!]}(\mathfrak{g})_{\mathbb{Z}_{(p)}}$.

One can now compute that, for $\alpha, \beta \in \Phi$, $1 \leqslant t, t_1, t_2 \leqslant d$ and $0 \leqslant s, u < r+1$, we have

$$\left[\mathbf{e}_\alpha^{(p^s)}, \mathbf{e}_\beta^{(p^u)}\right] \in \widetilde{U}^{[\![r]\!]}(\mathfrak{g})_{\mathbb{Z}_{(p)}},$$

$$\left[\mathbf{e}_\alpha^{(p^s)}, \mathbf{e}_{-\alpha}^{(p^u)}\right] \in \widetilde{U}^{[\![r]\!]}(\mathfrak{g})_{\mathbb{Z}_{(p)}},$$

$$\left[\mathbf{e}_\alpha^{(p^s)}, \binom{\mathbf{h}_t}{p^u}\right] = \sum_{l=0}^{p^u-1} \binom{-\alpha(\mathbf{h}_t)p^s}{p^u - l} \binom{\mathbf{h}_t}{l} \mathbf{e}_\alpha^{(p^s)} \in \widetilde{U}^{[\![r]\!]}(\mathfrak{g})_{\mathbb{Z}_{(p)}},$$

$$\left[\binom{\mathbf{h}_{t_1}}{p^s}, \binom{\mathbf{h}_{t_2}}{p^u}\right] = 0.$$

More specifically, we know that when we write these commutators in the divided powers basis we have coefficients in $\mathbb{Z}_{(p)}$ (this just follows from $\widetilde{U}(\mathfrak{g})_{\mathbb{Z}_{(p)}}$ being a $\mathbb{Z}_{(p)}$-form). Hence, for the above statements to hold, all we have to show is that none of the divided power indices exceed $p^{r+1}-1$. The first two of these calculations can be checked directly using [Kostant, 1966] and Lemma 15 in [Steinberg, 1968], while the second two are clear. For example, if $\{\alpha, \beta\}$ form the fundamental roots for a root system of type G_2 with β the long root, then we have

$$\left[\mathbf{e}_\alpha^{(p^s)}, \mathbf{e}_\beta^{(p^u)}\right] = \sum \epsilon_{k_1,k_2,k_3,k_4} \mathbf{e}_\beta^{(p^u-k_1-k_2-k_3-2k_4)} \left(\prod_{j=1}^{3} \mathbf{e}_{j\alpha+\beta}^{(k_j)}\right) \cdot \mathbf{e}_{3\alpha+2\beta}^{(k_4)} \mathbf{e}_\alpha^{(p^s-k_1-2k_2-3k_3-3k_4)}$$

where the sum is over all $k_1, k_2, k_3, k_4 \geqslant 0$, not all zero, such that $k_1+k_2+k_3+2k_4 \leqslant p^s$ and $k_1+2k_2+3k_3+3k_4 \leqslant p^u$ and $\epsilon_{k_1,k_2,k_3,k_4} \in \mathbb{Z}$ for all k_1, k_2, k_3, k_4. In particular, none of the heights of the divided powers are greater than or equal to p^{r+1}. The rest are similar. □

We can hence form $U^{[\![r]\!]}(\mathfrak{g}) := U^{[\![r]\!]}(\mathfrak{g})_{\mathbb{Z}_{(p)}} \otimes_{\mathbb{Z}_{(p)}} \mathbb{K}$.

Proposition 3.3.2.2. *There is an isomorphism of algebras $U^{[\![r]\!]}(\mathfrak{g}) \cong U^{[r]}(G)$.*

Proof. We prove this by constructing an algebra homomorphism $U^{[r]}(G) \to U^{[\![r]\!]}(\mathfrak{g})$ using the universal property and showing that it sends a basis of $U^{[r]}(G)$ to a basis of $U^{[\![r]\!]}(\mathfrak{g})$.

$\mathrm{Dist}_{p^{r+1}-1}(G)$ has $\mathbb{K}$-basis

$$\left\{ \prod_{\alpha\in\Phi^+} \mathbf{e}_\alpha^{(i_\alpha)} \prod_{t=1}^{d} \binom{\mathbf{h}_t}{k_t} \prod_{\alpha\in\Phi^+} \mathbf{e}_{-\alpha}^{(j_\alpha)} \;:\; \sum_{\alpha\in\Phi^+} (i_\alpha + j_\alpha) + \sum_{t=1}^{d} k_t < p^{r+1} \right\}.$$

Define $\phi : \mathrm{Dist}_{p^{r+1}-1}(G) \to U^{\llbracket r \rrbracket}(\mathfrak{g})$ by

$$\phi\left(\prod_{\alpha\in\Phi^+}\mathbf{e}_\alpha^{(i_\alpha)}\prod_{t=1}^{d}\binom{\mathbf{h}_t}{k_t}\prod_{\alpha\in\Phi^+}\mathbf{e}_{-\alpha}^{(j_\alpha)}\right) = \prod_{\alpha\in\Phi^+}\mathbf{e}_\alpha^{(i_\alpha)}\prod_{t=1}^{d}\binom{\mathbf{h}_t}{k_t}\prod_{\alpha\in\Phi^+}\mathbf{e}_{-\alpha}^{(j_\alpha)}.$$

The fact that $\phi(\delta\rho) = \phi(\delta)\phi(\rho)$ if $\delta \in \mathrm{Dist}_i^+(G)$, $\rho \in \mathrm{Dist}_j^+(G)$ with $i + j < p^{r+1}$ and $\phi([\delta, \rho]) = [\phi(\delta), \phi(\rho)]$ if $\delta \in \mathrm{Dist}_i^+(G)$, $\rho \in \mathrm{Dist}_j^+(G)$ with $i + j \leqslant p^{r+1}$ is obvious from how basis elements in $\mathrm{Dist}_{p^{r+1}-1}(G)$ multiply (since below the p^{r+1} level, the multiplication is the same in $U^{\llbracket r \rrbracket}(\mathfrak{g})$ and $\mathrm{Dist}(G)$). Hence we get an algebra homomorphism $\phi : U^{[r]}(G) \to U^{\llbracket r \rrbracket}(\mathfrak{g})$ from the universal property.[75]

We now need some notation for the elements in $U^{[r]}(G)$. Given an integer $M = a_0 + a_1 p + \cdots + a_r p^r$ where $0 \leqslant a_0, \ldots, a_{r-1} < p$ and $a_r \geqslant 0$, we define

$$\mathbf{e}_\alpha^{\llbracket M \rrbracket_\otimes} = \mathbf{e}_\alpha^{\otimes a_0} \otimes (\mathbf{e}_\alpha^{(p)})^{\otimes a_1} \otimes \cdots \otimes (\mathbf{e}_\alpha^{(p^r)})^{\otimes a_r} \in U^{[r]}(G)$$

for $\alpha \in \Phi$. Furthermore, define

$$\binom{\mathbf{h}_t}{\llbracket M \rrbracket_\otimes} = \binom{\mathbf{h}_t}{1}^{\otimes a_0} \otimes \binom{\mathbf{h}_t}{p}^{\otimes a_1} \otimes \cdots \otimes \binom{\mathbf{h}_t}{p^r}^{\otimes a_r} \in U^{[r]}(G)$$

for $1 \leqslant t \leqslant d$. Then

$$\phi\Big(\bigotimes_{\alpha\in\Phi^+}\mathbf{e}_\alpha^{\llbracket i_\alpha \rrbracket_\otimes}\bigotimes_{t=1}^{d}\binom{\mathbf{h}_t}{\llbracket k_t \rrbracket_\otimes}\bigotimes_{\alpha\in\Phi^+}\mathbf{e}_{-\alpha}^{\llbracket j_\alpha \rrbracket_\otimes}\Big) = \prod_{\alpha\in\Phi^+}\mathbf{e}_\alpha^{\llbracket i_\alpha \rrbracket}\prod_{t=1}^{d}\binom{\mathbf{h}_t}{\llbracket k_t \rrbracket}\prod_{\alpha\in\Phi^+}\mathbf{e}_{-\alpha}^{\llbracket j_\alpha \rrbracket}.$$

Furthermore, it is not difficult to see that the

$$\bigotimes_{\alpha\in\Phi^+}\mathbf{e}_\alpha^{\llbracket i_\alpha \rrbracket_\otimes}\bigotimes_{t=1}^{d}\binom{\mathbf{h}_t}{\llbracket k_t \rrbracket_\otimes}\bigotimes_{\alpha\in\Phi^+}\mathbf{e}_{-\alpha}^{\llbracket j_\alpha \rrbracket_\otimes},$$

for $i_\alpha, j_{-\alpha}, k_t \in \mathbb{N}$, span $U^{[r]}(G)$ as a vector space. They are also linearly independent, since their images under the map ϕ are. Thus, ϕ maps a basis to a basis, and the result holds.

□

Hence $U^{\llbracket r \rrbracket}(\mathfrak{g}) \cong U^{[r]}(G)$ as algebras and $U^{[r]}(G)$ has the desired basis, which we generally abuse notation to denote it as

$$\left\{\prod_{\alpha\in\Phi^+}\mathbf{e}_\alpha^{\llbracket i_\alpha \rrbracket}\prod_{t=1}^{d}\binom{\mathbf{h}_t}{\llbracket k_t \rrbracket}\prod_{\alpha\in\Phi^+}\mathbf{e}_{-\alpha}^{\llbracket j_\alpha \rrbracket} \quad : \quad 0 \leqslant i_\alpha, j_\alpha, k_t\right\}.$$

Note that the universal property of $U(\mathfrak{g})$ gives a $\mathbb{K}$-algebra homomorphism $U(\mathfrak{g}) \to U^{[0]}(G)$. This basis guarantees that this is an isomorphism of $\mathbb{K}$-algebras.[76]

[75] Recall Proposition 3.2.1.1.

[76] In fact, this is an isomorphism of Hopf algebras, by considering the effect of the comultiplication, counit and antipode on the corresponding bases.

Hence, the representation theory of reductive Lie algebras over a field of characteristic $p > 0$ as studied in the papers [Friedlander and Parshall, 1988] and [Friedlander and Parshall, 1990] exists within our theory as the case when $r = 0$. One can also see this using Kaneda and Ye's construction $\mathbb{U}^{(0)}$ and Proposition 3.4.2.1, *infra.*

With this basis of $U^{[r]}(G)$ in place, we can now prove the following proposition.

Proposition 3.3.2.3. *If G is reductive, the image of ξ_r is central in $U^{[r]}(G)$.*

Proof. By Lemma 3.3.1.2 and Proposition 3.3.1.3, it is enough to show that $\xi_r(\mathbf{e}_\alpha^{(p^r)})$ and $\xi_r(\binom{\mathbf{h}_t}{p^r})$ are central for $\alpha \in \Phi$ and $1 \leqslant t \leqslant d$. We know that $\xi_r(\mathbf{e}_\alpha^{(p^r)}) = (\mathbf{e}_\alpha^{(p^r)})^{\otimes p}$ and $\xi_r(\binom{\mathbf{h}_t}{p^r}) = \binom{\mathbf{h}_t}{p^r}^{\otimes p} - \binom{\mathbf{h}_t}{p^r}$. By the given basis of $U^{[r]}(G)$, it is enough to show that $\xi_r(\mathbf{e}_\alpha^{(p^r)})$ and $\xi_r(\binom{\mathbf{h}_t}{p^r})$ commute with each element of $\mathrm{Dist}^+_{p^r}(G)$.

Observe that in the notation coming from the $\mathbb{Z}_{(p)}$-form the multiplicative notation means the tensor product notation in $U^{[r]}(G)$. This gives us that for $\alpha, \beta \in \Phi$ with $\alpha \neq -\beta$ and $0 < s \leqslant r$, Lemma 15 in [Steinberg, 1968] shows

$$\left[(\mathbf{e}_\alpha^{(p^r)})^p, \mathbf{e}_\beta^{(p^s)}\right] = \frac{p^{r+1}!}{(p^r!)^p}\left[\mathbf{e}_\alpha^{(p^{r+1})}, \mathbf{e}_\beta^{(p^s)}\right] \in \frac{p^{r+1}!}{(p^r!)^p} U^{[\![r]\!]}(\mathfrak{g})_{\mathbb{Z}_{(p)}},$$

$$\left[(\mathbf{e}_\alpha^{(p^r)})^p, \mathbf{e}_{-\alpha}^{(p^s)}\right] = \frac{p^{r+1}!}{(p^r!)^p}\left[\mathbf{e}_\alpha^{(p^{r+1})}, \mathbf{e}_{-\alpha}^{(p^s)}\right] \in \frac{p^{r+1}!}{(p^r!)^p} U^{[\![r]\!]}(\mathfrak{g})_{\mathbb{Z}_{(p)}}.$$

In fact, comparing coefficients in the equation from [Steinberg, 1968, Lemma 15] shows that these commutators lie in $\frac{p^{r+1}!}{(p^r!)^p}\widetilde{U}^{[\![r]\!]}(\mathfrak{g})_{\mathbb{Z}_{(p)}}$, not just in $\frac{p^{r+1}!}{(p^r!)^p}U^{[\![r]\!]}(\mathfrak{g})_{\mathbb{Z}_{(p)}}$. The reader can see this with the observation that if, for example, $\{\alpha, \beta\}$ form the fundamental roots for a root system of type G_2 with β the long root, then we have that

$$\left[\mathbf{e}_\alpha^{(p^{r+1})}, \mathbf{e}_\beta^{(p^s)}\right] = \sum \epsilon_{k_1,k_2,k_3,k_4} \mathbf{e}_\beta^{(p^s-k_1-k_2-k_3-2k_4)} \left(\prod_{j=1}^{3} \mathbf{e}_{j\alpha+\beta}^{(k_j)}\right) \cdot \mathbf{e}_{3\alpha+2\beta}^{(k_4)} \mathbf{e}_\alpha^{(p^{r+1}-k_1-2k_2-3k_3-3k_4)}$$

where the sum is over all $k_1, k_2, k_3, k_4 \geqslant 0$, not all zero, such that $k_1+k_2+k_3+2k_4 \leqslant p^{r+1}$ and $k_1 + 2k_2 + 3k_3 + 3k_4 \leqslant p^s$ and $\epsilon_{k_1,k_2,k_3,k_4} \in \mathbb{Z}$ for all k_1, k_2, k_3, k_4. In particular, none of the divided powers are greater than or equal to p^{r+1}.

Since $\frac{p^{r+1}!}{(p^r!)^p} \in \mathbb{Z}$ vanishes modulo p, the above equations hence show that the commutators vanish in $U^{[\![r]\!]}(\mathfrak{g}) = U^{[\![r]\!]}(\mathfrak{g})_{\mathbb{Z}_{(p)}} \otimes_{\mathbb{Z}_{(p)}} \mathbb{K}$.

Furthermore,

$$\left[(\mathbf{e}_\alpha^{(p^r)})^p, \binom{\mathbf{h}_t}{p^s}\right] = \sum_{l=0}^{p^s-1} \binom{-\alpha(\mathbf{h}_t)p^{r+1}}{p^s - l}\binom{\mathbf{h}_t}{l}(\mathbf{e}_\alpha^{(p^r)})^p = 0,$$

where the last equality follows from the observation that $\binom{-\alpha(\mathbf{h}_t)p^{r+1}}{p^s-l} = 0$ modulo p

for all $0 \leqslant l \leqslant p^s - 1$. This comes from Lucas' Theorem[77] and the fact that $s < r+1$. This gives the centrality of $\xi_r(\mathbf{e}_\alpha^{(p^r)})$. For $\xi_r(\binom{\mathbf{h}_t}{p^r})$ we have

$$\left[\binom{\mathbf{h}_t}{p^r}^{\otimes p} - \binom{\mathbf{h}_t}{p^r}, \binom{\mathbf{h}_u}{p^s}\right] = 0$$

and

$$\begin{aligned}
\left(\binom{\mathbf{h}_t}{p^r}^{\otimes p} - \binom{\mathbf{h}_t}{p^r}\right)\mathbf{e}_\alpha^{(p^s)} &= \mathbf{e}_\alpha^{(p^s)}\left(\binom{\mathbf{h}_t - \alpha(\mathbf{h}_t)p^s}{p^r}^{\otimes p} - \binom{\mathbf{h}_t - \alpha(\mathbf{h}_t)p^s}{p^r}\right) \\
&= \mathbf{e}_\alpha^{(p^s)}\left(\left(\sum_{l=0}^{p^r}\binom{\mathbf{h}_t}{l}\binom{-\alpha(\mathbf{h}_t)p^s}{p^r - l}\right)^{\otimes p} - \sum_{l=0}^{p^r}\binom{\mathbf{h}_t}{l}\binom{-\alpha(\mathbf{h}_t)p^s}{p^r - l}\right) \\
&= \mathbf{e}_\alpha^{(p^s)}\left(\sum_{l=0}^{p^r}\binom{\mathbf{h}_t}{l}^{\otimes p}\binom{-\alpha(\mathbf{h}_t)p^s}{p^r - l} - \sum_{l=0}^{p^r}\binom{\mathbf{h}_t}{l}\binom{-\alpha(\mathbf{h}_t)p^s}{p^r - l}\right) \\
&= \mathbf{e}_\alpha^{(p^s)}\left(\binom{\mathbf{h}_t}{p^r}^{\otimes p} - \binom{\mathbf{h}_t}{p^r}\right)
\end{aligned}$$

since $\binom{\mathbf{h}_t}{l}^{\otimes p} = \binom{\mathbf{h}_t}{l}$ for $l < p^r$. This gives the centrality of $\xi_r(\binom{\mathbf{h}_t}{p^r})$. Hence the image of ξ_r is central.

□

This proposition finally allows us to prove the following result for higher universal enveloping algebras of arbitrary affine algebraic groups. The idea for this proof is due to Lewis Topley.

Corollary 3.3.2.4. *Let G be an affine algebraic group. For $\delta \in \mathrm{Dist}^+_{p^r}(G)$, the element $\delta^{\otimes p} - \delta^p$ is central in $U^{[r]}(G)$.*

Proof. If G is an affine algebraic group, then there is an inclusion $\mathrm{Dist}(G) \subseteq \mathrm{Dist}(\mathrm{GL}_m)$ for some $m \in \mathbb{N}$, which restricts to an inclusion $\mathrm{Dist}_k(G) \subseteq \mathrm{Dist}_k(\mathrm{GL}_m)$ for all $k \in \mathbb{N}$. In particular, the inclusion $\mathrm{Dist}^+_{p^{r+1}-1}(G) \hookrightarrow \mathrm{Dist}^+_{p^{r+1}-1}(\mathrm{GL}_m) \hookrightarrow U^{[r]}(\mathrm{GL}_m)$ induces, by the universal property, an algebra homomorphism

$$\iota : U^{[r]}(G) \to U^{[r]}(\mathrm{GL}_m).$$

Let $x_1, \ldots, x_n$ be a basis of $\mathfrak{g} = \mathrm{Lie}(G)$. This can be extended to a basis $x_1 \ldots, x_{m^2}$ of $\mathfrak{gl}_m = \mathrm{Lie}(\mathrm{GL}_m)$.

The map ι sends

$$x_1^{(a_1)}x_2^{(a_2)}\ldots x_n^{(a_n)}(x_1^{(p^r)})^{b_1}(x_2^{(p^r)})^{b_2}\ldots(x_n^{(p^r)})^{b_n} \in U^{[r]}(G)$$

[77]**Lucas' Theorem:** If $a, b \in \mathbb{Z}$ with $a = a_0+b_1p+a_2p^2+\cdots a_kp^k$ and $b = b_0+b_1p+b_2p^2+\cdots+b_kp^k$ for $0 \leqslant a_i, b_i < p$, then $\binom{a}{b}$ is congruent mod p to $\binom{a_0}{b_0}\binom{a_1}{b_1}\binom{a_2}{b_2}\ldots\binom{a_k}{b_k}$. In particular, if $b_i > a_i$ for some $0 \leqslant i \leqslant k$ then $\binom{a}{b} = 0$.

to
$$x_1^{(a_1)}x_2^{(a_2)}\dots x_n^{(a_n)}(x_1^{(p^r)})^{b_1}(x_2^{(p^r)})^{b_2}\dots(x_n^{(p^r)})^{b_n}\in U^{[r]}(\mathrm{GL}_m).$$

Hence, by Corollary 3.3.1.8, ι is injective.

In particular, there is an inclusion $\iota : U^{[r]}(G) \hookrightarrow U^{[r]}(\mathrm{GL}_m)$. Now, for $\delta \in \mathrm{Dist}^+_{p^r}(G)$, the element $\iota(\delta)^{\otimes p} - \iota(\delta)^p$ is central in $U^{[r]}(\mathrm{GL}_m)$ by Proposition 3.3.2.3, since GL_m is reductive.

Hence, $\delta^{\otimes p} - \delta^p$ is central in $U^{[r]}(G)$. □

3.4 Affine algebraic groups

3.4.1 Centres

Let G be an affine algebraic group with Lie algebra $\mathfrak{g}$, and let $x_1, \dots, x_n$ be a basis of $\mathfrak{g}$. We define by $Z_p^{[r]}$ the subalgebra of $Z(U^{[r]}(G))$ generated by the $\xi_r(\delta)$ for $\delta \in \mathrm{Dist}^+_{p^r}(G)$. Using Corollaries 3.3.1.8 and 3.3.2.4, we can easily see that $Z_p^{[r]}$ is generated by $(x_i^{(p^r)})^{\otimes p} - (x_i^{(p^r)})^p$ for $i = 1, \dots, n$. From Corollary 3.3.1.8, it is clear that these elements are algebraically independent over $\mathbb{K}$.

Note the semilinearity of ξ_r induces an algebra homomorphism from $S(Y^{(1)}_{p^r})$ (the symmetric algebra on the vector space $Y^{(1)}_{p^r}$ defined above) to $Z_p^{[r]}$. This map is bijective.

As a $Z_p^{[r]}$-module under left multiplication, $U^{[r]}(G)$ is free of rank $p^{(r+1)\dim(\mathfrak{g})}$, with free basis
$$\{x_1^{(a_1)}x_2^{(a_2)}\dots x_n^{(a_n)} \mid 0 \leqslant a_1, \dots, a_n < p^{r+1}\}.$$

If G is reductive, we can write this free basis as
$$\left\{ \prod_{\alpha\in\Phi^+} \mathbf{e}_\alpha^{[\![i_\alpha]\!]} \prod_{\beta\in\Pi} \binom{\mathbf{h}_\beta}{[\![k_\beta]\!]} \prod_{\alpha\in\Phi^+} \mathbf{e}_{-\alpha}^{[\![j_\alpha]\!]} \;\middle|\; 0 \leqslant i_\alpha, j_\alpha, k_\beta < p^{r+1} \right\}.$$

This leads us to the following proposition.

Proposition 3.4.1.1. *The centre $Z(U^{[r]}(G))$ of $U^{[r]}(G)$ is a finitely generated algebra over $\mathbb{K}$. As a $Z(U^{[r]}(G))$-module, $U^{[r]}(G)$ is finitely generated.*

Theorem 3.4.1.2. *Let E be an irreducible $U^{[r]}(G)$-module. Then E is finite-dimensional, of dimension less than or equal to $p^{(r+1)\dim(\mathfrak{g})}$.*

Proof. This follows in exactly the same way as Theorem A.4 in [Jantzen, 2004]. □

3.4.2 Comparison with Kaneda-Ye construction

Let G be a reductive algebraic group. Recall that Kaneda and Ye[78] construct the algebra

$$\mathbb{U}^{(r)} := \frac{T_{\mathbb{K}}(\mathrm{Dist}_{2p^r-1}(G))}{\left\langle \begin{array}{c} \lambda - \lambda\varepsilon_G,\ \delta\otimes\delta' - \delta'\otimes\delta - [\delta,\delta'],\ \delta\otimes\delta'' - \delta\delta'' \\ \text{where } \lambda \in \mathbb{K},\ \delta'' \in \mathrm{Dist}_{p^r-1}(G),\ \delta,\delta' \in \mathrm{Dist}_{p^r}(G) \end{array} \right\rangle},$$

with ε_G the counit of G.

Proposition 3.4.2.1. *The algebras $\mathbb{U}^{(r)}$ and $U^{[r]}(G)$ are isomorphic.*

Proof. The algebra $\mathbb{U}^{(r)}$ has a clear universal property, which causes the inclusion $\mathrm{Dist}_{2p^r-1}(G) \hookrightarrow U^{[r]}(G)$ to induce an algebra homomorphism $\mathbb{U}^{(r)} \to U^{[r]}(G)$. The surjectivity of this homomorphism is obvious from the basis constructed in Chapter 3.3.2.

It is left as an exercise for the reader to show that the proof of Proposition 3.3.2.2, showing that the algebra $U^{[r]}(G)$ has the given basis, applies equally well to the algebra $\mathbb{U}^{(r)}$. This guarantees that the algebra homomorphism $\mathbb{U}^{(r)} \to U^{[r]}(G)$ is an isomorphism. □

3.5 Higher reduced enveloping algebras

3.5.1 Deformation algebras

In this section we start to consider the representation theory of the algebra $U^{[r]}(G)$. From Proposition 3.2.1.3, we have the immediate result:

Corollary 3.5.1.1. *There is a bijection between the set of (isomorphism classes of) indexed $\mathrm{Dist}^+_{p^{r+1}-1}(G)$-modules and the set of (isomorphism classes of) $U^{[r]}(G)$-modules.*

One of the most important differences between the representation theory of Lie algebras in characteristic zero and in positive characteristic is the fact that in characteristic $p > 0$ all irreducible representations of $U(\mathfrak{g})$ are finite-dimensional. Theorem 3.4.1.2 tells us that we can conclude a similar result for irreducible $U^{[r]}(G)$-modules. The natural question to ask is: how much of the representation theory of $U(\mathfrak{g})$ can be similarly extended to develop the representation theory of $U^{[r]}(G)$? To that end, let us follow the path well-trodden in the $r = 0$ case and see how many difficulties we discover in the generalisation.

Suppose that E is an irreducible $U^{[r]}(G)$-module. It is finite-dimensional by Theorem 3.4.1.2. Hence, by Schur's lemma, $\xi_r(\delta) \in Z_p^{[r]}$ acts as a scalar on E for

[78]See [Kaneda and Ye, 2007].

each $\delta \in \mathrm{Dist}^+_{p^r}(G)$. By the semilinearity of ξ_r, we can deduce that there exists $\chi_E \in \mathrm{Dist}^+_{p^r}(G)^*$ (the vector space dual) such that

$$\xi_r(\delta)|_E = \chi_E(\delta)^p \mathrm{Id}_E \qquad \text{for all } \delta \in \mathrm{Dist}^+_{p^r}(G).$$

Note that $\chi_E(\delta) = 0 \iff \chi_E(\delta)^p = 0 \iff \xi_r(\delta)|_E = 0$. In particular, this means that $\chi_E(X_{p^r}) = 0$, where X_{p^r} is defined as in Subsection 3.3.1.

Recall from Proposition 3.2.2.1 and Corollary 3.2.2.3 that $\Upsilon_{r,r} : U^{[r]}(G) \to U(\mathfrak{g})^{(r)}$ is a surjective algebra homomorphism such that $\Upsilon_{r,r}(\mathrm{Dist}^+_{p^r}(G)) = \mathfrak{g}^{(r)}$. The linear map $\Upsilon_{r,r}|_{\mathrm{Dist}^+_{p^r}(G)} \colon \mathrm{Dist}^+_{p^r}(G) \to \mathfrak{g}^{(r)}$ (in fact indexed algebra subspace homomorphism) has kernel X_{p^r} and hence χ_E passes to a linear map $\hat{\chi}_E \colon \mathfrak{g} \to \mathbb{K}$. Similarly, given $(\hat{\chi} \in \mathfrak{g}^*)^{(r)}$ we can extend along $\Upsilon_{r,r}|_{\mathrm{Dist}^+_{p^r}(G)}$ to get a linear form $\chi : \mathrm{Dist}^+_{p^r}(G) \to \mathbb{K}$. We abuse notation slightly in the following way: given $(\chi \in \mathfrak{g}^*)^{(r)}$, we also denote by χ the linear form $\mathrm{Dist}^+_{p^r}(G) \to \mathbb{K}$ induced by $\Upsilon_{r,r}$.[79]

This allows us to make the following definition for $(\chi \in \mathfrak{g}^*)^{(r)}$:

$$U^{[r]}_\chi(G) := \frac{U^{[r]}(G)}{\langle \xi_r(\delta) - \chi(\delta)^p \mid \delta \in \mathrm{Dist}^+_{p^r}(G) \rangle}.$$

We call such an algebra a **higher reduced enveloping algebra**. Since all irreducible $U^{[r]}(G)$-modules are finite-dimensional by Theorem 3.4.1.2, Schur's lemma allows us to easily deduce the following result.

Proposition 3.5.1.2. *Every irreducible $U^{[r]}(G)$-module is a $U^{[r]}_\chi(G)$-module for some $\chi \in \mathfrak{g}^*$.*

It is straightforward to show that as a vector space over $\mathbb{K}$ this algebra has dimension $p^{(r+1)\dim(\mathfrak{g})}$ with basis the classes of

$$\{x_1^{(a_1)} x_2^{(a_2)} \dots x_n^{(a_n)} \mid 0 \leqslant a_i < p^{r+1} \text{ for all } 1 \leqslant i \leqslant n\}$$

in $U^{[r]}_\chi(G)$. When G is reductive, the basis can be written as the classes of

$$\left\{ \prod_{\alpha \in \Phi^+} \mathbf{e}_\alpha^{[\![i_\alpha]\!]} \prod_{t=1}^{d} \binom{\mathbf{h}_t}{[\![k_t]\!]} \prod_{\alpha \in \Phi^+} \mathbf{e}_{-\alpha}^{[\![j_\alpha]\!]} \;\middle|\; 0 \leqslant i_\alpha, j_\alpha, k_t < p^{r+1} \right\}$$

in $U^{[r]}_\chi(G)$. At times, it will also be beneficial to consider another basis of this algebra, which can be derived easily from properties of divided powers. This basis consists of the classes of

$$\left\{ \prod_{\alpha \in \Phi^+} \mathbf{e}_\alpha^{(i_\alpha)} \prod_{t=1}^{d} \binom{\mathbf{h}_t}{k_t} \prod_{\alpha \in \Phi^+} \mathbf{e}_{-\alpha}^{(j_\alpha)} \;\middle|\; 0 \leqslant i_\alpha, j_\alpha, k_t < p^{r+1} \right\}$$

[79]Since $\mathfrak{g}^*$ and $(\mathfrak{g}^*)^{(r)}$ are equal as sets (and as G-sets) we generally just write $\mathfrak{g}^*$ unless the vector space structure is of particular importance.

in $U_\chi^{[r]}(G)$.

We saw as a result of Corollary 3.3.1.5 that $U_0^{[r]}(G) = \mathrm{Dist}(G_{r+1})$. One can also show that, for $\chi \in \mathfrak{g}^*$ and $s \leqslant r$, we get that $\Upsilon_{r,r-s} \colon U_\chi^{[r]}(G) \to U_\chi^{[s]}(G)^{(r-s)}$ is a well-defined algebra homomorphism. So we get the sequence of algebra homomorphisms

$$U_\chi^{[r]}(G) \twoheadrightarrow U_\chi^{[r-1]}(G)^{(1)} \twoheadrightarrow \cdots \twoheadrightarrow U_\chi^{[1]}(G)^{(r-1)} \twoheadrightarrow U_\chi(\mathfrak{g})^{(r)}.$$

Given $g \in G$, we get an adjoint action of g, denoted $\mathrm{Ad}(g)$, on $\mathrm{Dist}^+_{p^r}(G)$. This leads to a coadjoint action of g on $\mathrm{Dist}^+_{p^r}(G)^*$. We furthermore have a twisted coadjoint action of g on $(\mathfrak{g}^*)^{[r]}$, corresponding to the twisted adjoint action $\mathrm{Ad}(F^r(g))$.

Lemma 3.5.1.3. *Given $(\chi \in \mathfrak{g}^*)^{[r]}$ and $g \in G$, there is an isomorphism $U_\chi^{[r]}(G) \cong U_{g\cdot\chi}^{[r]}(G)$.*

Proof. Consider the coadjoint actions of G on $\mathrm{Dist}^+_{p^r}(G)^*$ and on $\mathfrak{g}^*$ (untwisted and twisted respectively). A priori, the actions need not be compatible when we switch between considering $(\chi \in \mathfrak{g}^*)^{[r]}$ as a linear form on $\mathfrak{g}$ and a linear form on $\mathrm{Dist}^+_{p^r}(G)$. However, the G-equivariance of $\Upsilon_{r,r}$ (see Lemma 3.2.2.2) means that this is not a problem – the actions are compatible.

As a result, one can show that $U_\chi^{[r]}(G) \cong U_{g\cdot\chi}^{[r]}(G)$ where we mean by $g \cdot \chi$ the (twisted) coadjoint action of g on χ - by Subsection 3.2.2, it doesn't matter here if we consider the action of g on $(\chi \in \mathfrak{g}^*)^{[r]}$ or $\chi \in \mathrm{Dist}^+_{p^r}(G)^*$. □

In particular, much like in the $r = 0$ case, to understand the representation theory of $U^{[r]}(G)$ it is enough to understand the representation theory of $U_\chi^{[r]}(G)$ for $(\chi \in \mathfrak{g}^*)^{[r]}$ in distinct G-orbits.

3.5.2 Frobenius kernels

We would now like to show that $\mathrm{Dist}(G_r)$ is a subalgebra of $U_\chi^{[r]}(G)$ for any choice of $\chi \in \mathfrak{g}^*$. We saw earlier[80] that

$$\mathrm{Dist}(G_r) \cong \frac{U^{[r]}(G)}{\langle \delta^{\otimes p} - \delta^p \mid \delta \in \mathrm{Dist}^+_{p^{r-1}}(G)\rangle}$$

so by induction it is enough to construct an injective algebra homomorphism

$$\frac{U^{[r-1]}(G)}{\langle \delta^{\otimes p} - \delta^p \mid \delta \in \mathrm{Dist}^+_{p^{r-1}}(G)\rangle} \hookrightarrow \frac{U^{[r]}(G)}{\langle \delta^{\otimes p} - \delta^p - \chi(\delta)^p 1 \mid \delta \in \mathrm{Dist}^+_{p^r}(G)\rangle}.$$

Inclusion gives us a map $i \colon \mathrm{Dist}^+_{p^r-1}(G) \hookrightarrow \mathrm{Dist}^+_{p^{r+1}-1}(G) \hookrightarrow U^{[r]}(G)$ which clearly satisfies all the conditions for the universal property, so we get an algebra homomorphism

$$\bar{i} \colon U^{[r-1]}(G) \to U^{[r]}(G) \twoheadrightarrow U_\chi^{[r]}(G).$$

[80]See Corollary 3.3.1.5 and the discussion following it.

It is straightforward to see from the basis description of $U^{[r]}(G)$ that $\mathrm{Im}(\bar{i}) \cap \langle \delta^{\otimes p} - \delta^p - \chi(\delta)^p 1 \mid \delta \in \mathrm{Dist}^+_{p^r}(G)\rangle = 0$, so we just need to show that $\ker(\bar{i}) = \langle \delta^{\otimes p} - \delta^p \mid \delta \in \mathrm{Dist}^+_{p^{r-1}}(G)\rangle$. This follows easily from the basis descriptions of $U^{[r-1]}(G)$ and $U^{[r]}(G)$ once we notice that $\bar{i}((x_j^{(p^{r-1})})^{\otimes p}) = (x_j^{(p^{r-1})})^p$ for $1 \leqslant j \leqslant n$.

In particular, we have the following diagram of injective and surjective algebra homomorphisms:

$$\begin{tikzcd}
\cdots \arrow[dr, two heads] & U^{[r-1]}(G) \arrow[dr, two heads] & U^{[r]}(G) \arrow[dr, two heads] & U^{[r+1]}(G) \arrow[dr, two heads] & \\
\cdots \arrow[r, hook] & \mathrm{Dist}(G_{r-1}) \arrow[u, hook] \arrow[r, hook] & \mathrm{Dist}(G_r) \arrow[u, hook] \arrow[r, hook] & \mathrm{Dist}(G_{r+1}) \arrow[u, hook] \arrow[r, hook] & \cdots
\end{tikzcd}$$

This hence provides us with a direct system $\ldots \to U^{[r-1]}(G) \to U^{[r]}(G) \to U^{[r+1]} \to \ldots$ with direct limit $\varinjlim U^{[r]}(G) = \mathrm{Dist}(G)$. From what we have already shown, we can use this to deduce some details of the module theory of $U_\chi^{[r]}(G)$.

Proposition 3.5.2.1. *Every $U_\chi^{[r]}(G)$-module is a $\mathrm{Dist}(G_s)$-module for all $0 \leqslant s \leqslant r$.*

Proposition 3.5.2.2. *Every $U_\chi^{[s]}(G)^{(r-s)}$-module can be lifted to a $U_\chi^{[r]}(G)$-module via $\Upsilon_{r,r-s}$.*

We can put these two results together in the following theorem. The proof follows easily from Subsection 3.2.2.

Proposition 3.5.2.3. *Let M be a $U_\chi^{[r]}(G)$-module. If M is lifted from a $U_\chi^{[s]}(G)^{(r-s)}$-module along $\Upsilon_{r,r-s}$ then $\mathrm{Dist}^+(G_s)M = 0$. On the other hand, if $\mathrm{Dist}^+(G_s)M = 0$, then M is a $U_\chi^{[s]}(G)^{(r-s)}$-module via a lifting along $\Upsilon_{r,r-s}$.*

3.5.3 Examples

Example 5. *Consider the additive algebraic group $G = \mathbb{G}_a$. We know from Example 3 in Subsection 2.3.4 that $\mathrm{Dist}_{p^{r+1}-1}(G)$ has basis $\gamma_1, \gamma_2, \ldots, \gamma_{p^{r+1}-1}$ and that in $\mathrm{Dist}(G)$ the multiplication is $\gamma_k\gamma_l = \binom{k+l}{k}\gamma_{k+l}$. Using these facts one can show that*

$$U^{[r]}(\mathbb{G}_a) = \frac{\mathbb{K}[t_0, t_1, \ldots, t_r]}{\langle t_i^p \,|\, 0 \leqslant i \leqslant r-1 \rangle}.$$

Furthermore, given $\chi \in \mathfrak{g}^* = \mathbb{K}$, we get

$$U_\chi^{[r]}(\mathbb{G}_a) = \frac{\mathbb{K}[t_0, t_1, \ldots, t_r]}{\langle t_r^p - \chi^p; t_i^p \,|\, 0 \leqslant i \leqslant r-1 \rangle} \cong \frac{\mathbb{K}[t]}{\langle t^p \rangle} \otimes \cdots \otimes \frac{\mathbb{K}[t]}{\langle t^p \rangle} \otimes \frac{\mathbb{K}[t]}{\langle t^p - \chi^p \rangle}.$$

Example 6. *Consider the multiplicative algebraic group $G = \mathbb{G}_m$. We know from Example 4 in Subsection 2.3.4 that $\mathrm{Dist}_{p^{r+1}-1}(G)$ has basis $\delta_1, \delta_2, \ldots, \delta_{p^{r+1}-1}$ and that in $\mathrm{Dist}(G)$ the multiplication is $\delta_k\delta_l = \sum_{i=0}^{\min(k,l)} \frac{(k+l-i)!}{(k-i)!(l-i)!i!}\delta_{k+l-i}$. Using these facts one can show that*

$$U^{[r]}(\mathbb{G}_m) = \frac{\mathbb{K}[t_0, t_1, \ldots, t_r]}{\langle t_i^p - t_i \,|\, 0 \leqslant i \leqslant r-1 \rangle}.$$

Furthermore, given $\chi \in \mathfrak{g}^* = \mathbb{K}$, we get

$$U_{\chi}^{[r]}(\mathbb{G}_m) = \frac{\mathbb{K}[t_0, t_1, \ldots, t_r]}{\langle t_r^p - t_r - \chi^p; t_i^p - t_i \,|\, 0 \leqslant i \leqslant r-1 \rangle} \cong \mathbb{K} \times \cdots \times \mathbb{K}$$

where there are rp copies of $\mathbb{K}$ in the final expression, since $t_i^p - t_i$ and $t_r^p - t_r - \chi^p$ are separable polynomials. This tells us that the algebra $U_{\chi}^{[r]}(\mathbb{G}_m)$ is semisimple.

Chapter 4

Higher Deformations - Representation Theory

In Chapter 3 we were successfully able to construct the higher universal enveloping algebra $U^{[r]}(G)$ and the family of higher reduced enveloping algebras $U_\chi^{[r]}(G)$ indexed by $\chi \in \mathfrak{g}^*$. We would like to understand the representation theory of the algebras $U_\chi^{[r]}(G)$. We do so in this chapter for reductive groups.

Throughout this chapter we will assume that G is a reductive algebraic group over an algebraically closed field $\mathbb{K}$ of characteristic $p > 0$ and maintain the standard notation for the various subgroups and other objects associated with it which can be found in Subsection 2.4.1. In particular, G is defined over $\mathbb{F}_p$ so as observed at the end of Subsection 3.2.2 we may employ the geometric Frobenius endomorphism instead of the Frobenius morphism where relevant in order to avoid twisting $\mathbb{K}$-structures. We do this without comment for the remainder of the chapter.

Furthermore, we make Assumption (R), which the reader should recall from Subsection 2.4.4 is the assumption that the abelian group $X(T)/p^r X(T)$ has a set of representatives $X_r'(T)$ with $X_r'(T) \subseteq X_r(T)$.

4.1 Representation theory of $U^{[r]}(G)$

4.1.1 Decomposition of $U^{[r]}(G)$-modules

Suppose P is an irreducible left $\mathrm{Dist}(G_r)$-module and M is an irreducible left $U^{[r]}(G)$-module. Then P is a left $\mathrm{Dist}(G_{r+1})$-module by Remark 8 in Subsection 2.4.4. Hence, as $U^{[r]}(G)$ surjects onto $\mathrm{Dist}(G_{r+1})$, we have that P can be extended to a $U^{[r]}(G)$-module.

We can also define a left $U^{[r]}(G)$-module structure on $\mathrm{Hom}_{G_r}(P, M)$ as follows:[81]

$$x \cdot \phi : z \mapsto \sum x_{(1)}\phi(S(x_{(2)})z) \qquad \text{for} \quad x \in U^{[r]}(G),\ z \in P,\ \phi \in \mathrm{Hom}_{G_r}(N, M),$$

[81]Since the Frobenius kernels are infinitesimal group schemes, there is no difference between G_r-modules and $\mathrm{Dist}(G_r)$-modules, or homomorphisms between them, so we often use the notions interchangeably. See Section I.8.6 in [Jantzen, 1987] for more details.

where here we are using the $U^{[r]}(G)$-module structure on P defined in the previous paragraph. It is a straightforward calculation that this makes $\mathrm{Hom}_{G_r}(P, M)$ into a $U^{[r]}(G)$-module, and that the ideal $U^{[r]}(G)\mathrm{Dist}^+(G_r)$ acts trivially upon it. Hence, $\mathrm{Hom}_{G_r}(P, M)$ has the structure of a $U(\mathfrak{g}) = U^{[r]}(G)/U^{[r]}(G)\mathrm{Dist}^+(G_r)$-module.

Putting these two observations together and again using the Hopf algebra structure of $U^{[r]}(G)$, we can define a $U^{[r]}(G)$-module structure on $P \otimes \mathrm{Hom}_{G_r}(P, M)$.[82] Furthermore, if $x \in \mathrm{Dist}(G_r)$, $z \in P$ and $\phi \in \mathrm{Hom}_{G_r}(P, M)$, then

$$\begin{aligned} x \cdot (z \otimes \phi) &= \sum x_{(1)} z \otimes x_{(2)} \phi \\ &= \sum x_{(1)} z \otimes \epsilon(x_{(2)}) \phi \\ &= (\sum x_{(1)} \epsilon(x_{(2)}) z) \otimes \phi) \\ &= xz \otimes \phi, \end{aligned}$$

using here that elements of $\mathrm{Dist}(G_r)$ act on $\mathrm{Hom}_{G_r}(P, M)$ via ϵ, the counit. So we see that the $U^{[r]}(G)$-module structure on $P \otimes \mathrm{Hom}_{G_r}(P, M)$ restricts to the $\mathrm{Dist}(G_r)$-module structure on copies of P.

Theorem 4.1.1.1. *Make Assumption (R). Let M be an irreducible $U^{[r]}(G)$-module. Then there exists an irreducible $\mathrm{Dist}(G_r)$-module P such that $M \cong P \otimes \mathrm{Hom}_{G_r}(P, M)$ as $U^{[r]}(G)$-modules.*

Proof. Let P be an irreducible $\mathrm{Dist}(G_r)$-submodule of M. As above, we can equip $P \otimes \mathrm{Hom}_{G_r}(P, M)$ with the structure of a $U^{[r]}(G)$-module. We then define the map

$$\Psi : P \otimes \mathrm{Hom}_{G_r}(P, M) \to M, \qquad \Psi(z \otimes \phi) = \phi(z).$$

It is straightforward to check that this is a homomorphism of $U^{[r]}(G)$-modules. Since M is irreducible, it is clearly surjective. Hence, using Equation (4.1.1), as $\mathrm{Dist}(G_r)$-modules

$$M \cong \bigoplus_{i=1}^{k} P,$$

for some $k \in \mathbb{N}$. In particular, this implies that $\mathrm{Hom}_{G_r}(P, M) \cong \mathbb{K}^k$ and so $\dim_{\mathbb{K}}(M) = k \dim_{\mathbb{K}}(P)$. Furthermore, $\dim_{\mathbb{K}}(P \otimes \mathrm{Hom}_{G_r}(P, M)) = k \dim_{\mathbb{K}} P$. Hence, Ψ is an isomorphism. □

Theorem 4.1.1.1 therefore shows that an irreducible $U^{[r]}(G)$-module can be decomposed into an irreducible $\mathrm{Dist}(G_r)$-module and a $U(\mathfrak{g})$-module.

This result can also be obtained in a different way. This alternative method is more useful for the remainder of this chapter, and is inspired by the results of [Schneider, 1990] and [Witherspoon, 1999]. In particular, by Lemma 3.3.1.6, $\mathrm{Dist}(G_r) \subseteq U^{[r]}(G)$ is a $U(\mathfrak{g})$-Galois extension, so many of Schneider and Witherspoon's Clifford theoretic results are applicable in our setting.

[82] Recall from Subsection 2.2.1 that tensor product of two modules over a Hopf algebra H can be made into a module over H.

Lemma 4.1.1.2. *Make Assumption (R). Let P be an irreducible left* $\mathrm{Dist}(G_r)$*-module, and define the algebra*

$$E := \mathrm{End}_{U^{[r]}(G)}(U^{[r]}(G) \otimes_D P)^{op},$$

where here, and throughout this chapter, $D := \mathrm{Dist}(G_r)$. Let U be an irreducible left E-module. Then $P \otimes_{\mathbb{K}} U$ can be given a left $U^{[r]}(G)$-module structure which restricts to the natural left $\mathrm{Dist}(G_r)$*-module structure.*

Proof. The proof of this lemma can essentially be found in [Witherspoon, 1999], but we include elements of it here for ease of understanding. As described above, P can be extended to a $U^{[r]}(G)$-module. Remark 3.2(3) of [Schneider, 1990] shows that P is $U^{[r]}(G)$-stable.[83] It is proved in [Schneider, 1994] that $P \otimes_{\mathbb{K}} E$ is isomorphic to $U^{[r]}(G) \otimes_{\mathrm{Dist}(G_r)} P$ as right E-modules, using the $U^{[r]}(G)$-stability of P. In particular, by applying $- \otimes_E U$, this implies that

$$P \otimes_{\mathbb{K}} U \cong (U^{[r]}(G) \otimes_{\mathrm{Dist}(G_r)} P) \otimes_E U \tag{4.1}$$

can be given the structure of a left $U^{[r]}(G)$-module. Furthermore, Theorem 2.2(i) of [Witherspoon, 1999] shows that this $U^{[r]}(G)$-module structure restricts to the natural $\mathrm{Dist}(G_r)$-module structure.[84] □

Remark 9. *Lemma 4.1.1.2 gives another way to get a $U^{[r]}(G)$-module structure on $P \otimes \mathrm{Hom}_{G_r}(P, M)$, where M is an irreducible left $U^{[r]}(G)$-module, using the observation that $\mathrm{Hom}_{G_r}(P, M)$ is a left E-module.*[85]

The key point of the proof of Lemma 4.1.1.2 is Equation (4.1), which in the context of Remark 9 gives an isomorphism of $U^{[r]}(G)$-modules:

$$P \otimes \mathrm{Hom}_{G_r}(P, M) \cong (U^{[r]}(G) \otimes_D P) \otimes_E \mathrm{Hom}_{U^{[r]}(G)}(U^{[r]}(G) \otimes_D P, M).$$

It is straightforward to show that the map

$$\eta_M : (U^{[r]}(G) \otimes_D P) \otimes_E \mathrm{Hom}_{U^{[r]}(G)}(U^{[r]}(G) \otimes_D P, M) \to M,$$

$$\eta_M(a \otimes_D n \otimes_E \phi) = \phi(a \otimes_D n)$$

is a $U^{[r]}(G)$-module homomorphism, and a similar argument to Theorem 4.1.1.1 shows that it is an isomorphism. So we obtain the result:

Theorem 4.1.1.3. *Make Assumption (R). Let M be an irreducible $U^{[r]}(G)$-module. Then there exists an irreducible* $\mathrm{Dist}(G_r)$*-module P such that M is isomorphic to*

[83] This means that there exists a left $\mathrm{Dist}(G_r)$-linear and right $U(\mathfrak{g})$-collinear isomorphism $U^{[r]}(G) \otimes_{\mathrm{Dist}(G_r)} P \cong P \otimes_{\mathbb{K}} U(\mathfrak{g})$ - see, for example, [Schneider, 1990] or [Witherspoon, 1999] for the $U(\mathfrak{g})$-comodule structures on these spaces.

[84] Although Witherspoon's theorem is not directly applicable to this setting, it is observed in [Witherspoon, 1999] that the result still holds in the present situation.

[85] See, for example, Theorem 2.2.(ii) in [Witherspoon, 1999] for a proof of this statement.

$P \otimes \mathrm{Hom}_{\mathrm{Dist}(G_r)}(P, M)$ *as* $U^{[r]}(G)$*-modules, where the* $U^{[r]}(G)$*-module structure on* $P \otimes \mathrm{Hom}_{G_r}(P, M)$ *comes from Lemma 4.1.1.2.*

Remark 10. *Partial credit for this proof and that of Lemma 4.1.1.4,* infra*, goes to Dmitriy Rumynin, who was kind enough to share it with me.*

We observe in Remark 9 that $\mathrm{Hom}_{G_r}(P, M)$ is a left E-module. While at first blush the algebra E may appear strange, it turns out to be an algebra we know very well, as the following lemma shows.

Lemma 4.1.1.4. *Make Assumption (R). Let* $P \in \mathrm{Irr}(\mathrm{Dist}(G_r))$ *and*

$$E := \mathrm{End}_{U^{[r]}(G)}(U^{[r]}(G) \otimes_{\mathrm{Dist}(G_r)} P)^{op}.$$

Then $E \cong U(\mathfrak{g})$*.*

Proof. By Lemma 3.3.1.6, $\mathrm{Dist}(G_r) \subseteq U^{[r]}(G)$ is a $U(\mathfrak{g})$-Galois extension and $U^{[r]}(G)$ is faithfully flat as a right $\mathrm{Dist}(G_r)$-module. Furthermore, P is finitely-presented as a $\mathrm{Dist}(G_r)$-module (as both P and $\mathrm{Dist}(G_r)$ are finite-dimensional over $\mathbb{K}$), and $U(\mathfrak{g})$ is flat over $\mathbb{K}$ (as $\mathbb{K}$ is a field). Hence, we are in "Situation (S)" from [Schneider, 1990], so the results from that paper can be applied here. Theorem 3.6 in [Schneider, 1990] precisely states that $\mathbb{K} = \mathrm{End}_{\mathrm{Dist}(G_r)}(P)^{op} \subseteq E$ is a $U(\mathfrak{g})$-crossed product if and only if P is $U^{[r]}(G)$-stable, which holds under our assumptions as in the proof of Lemma 4.1.1.2. In particular, this means that there exists a right $U(\mathfrak{g})$-collinear, convolution invertible map $J : U(\mathfrak{g}) \to E$. More details about this map will be given in Remark 11 below. Thus, there exists a cocycle $\sigma : U(\mathfrak{g}) \otimes U(\mathfrak{g}) \to \mathbb{K}$ such that $E \cong \mathbb{K}\#_\sigma U(\mathfrak{g})$. The map $J : U(\mathfrak{g}) \to \mathbb{K}\#_\sigma U(\mathfrak{g}) \cong E$ (sending x to $1\#x$ in the first map) is clearly a bijection.

Furthermore, since the antipode of $U^{[r]}(G)$ is bijective (as $U^{[r]}(G)$ is cocommutative), Remark 3.8 in [Schneider, 1990] precisely says that J is an algebra homomorphism (i.e. $\mathbb{K} \subseteq E$ is a trivial $U(\mathfrak{g})$-crossed product) if and only if the $\mathrm{Dist}(G_r)$-module structure on P extends to a $U^{[r]}(G)$-module structure, which we have already seen to be true using Assumption (R). Hence $J : U(\mathfrak{g}) \to \mathbb{K}\#_\sigma U(\mathfrak{g}) \cong E$ is an isomorphism of algebras, as required. In particular, $E \cong \mathbb{K}\#U(\mathfrak{g})$.[86] ☐

Remark 11. *We can describe this isomorphism a little more explicitly. The isomorphism* $U(\mathfrak{g}) \cong \mathbb{K}\#U(\mathfrak{g})$ *sends* $x \in U(\mathfrak{g})$ *to* $1\#x \in \mathbb{K}\#U(\mathfrak{g})$*. We now need to consider the isomorphism* $\mathbb{K}\#U(\mathfrak{g}) \cong E$ *from [Schneider, 1990].*

Denoting $D := \mathrm{Dist}(G_r)$*, let* $q : U^{[r]}(G) \otimes_D P \to P$ *be the* $\mathrm{Dist}(G_r)$*-linear map extending the* $\mathrm{Dist}(G_r)$*-module structure on* P *to a* $U^{[r]}(G)$*-module structure. By Theorem 3.6 in [Schneider, 1990], there is a right* $U(\mathfrak{g})$*-collinear map* $J' : U(\mathfrak{g}) \to E$ *given by*

$$J'(h)(1 \otimes z) := \sum r_i(h) \otimes q(l_i(h) \otimes z),$$

[86] Here, $\mathbb{K}\#U(\mathfrak{g})$ means the **smash product** of $\mathbb{K}$ with $U(\mathfrak{g})$, which is precisely the crossed product with trivial cocycle. More details about smash products can be found in Chapter 4 in [Montgomery, 1993].

where $h \in U(\mathfrak{g})$, $z \in P$, and $r_i(h), l_i(h) \in U^{[r]}(G)$ are such that $\sum r_i(h) \otimes_D l_i(h)$ is the inverse image of $1 \otimes h$ under the canonical isomorphism

$$\mathrm{can} : U^{[r]}(G) \otimes_D U^{[r]}(G) \xrightarrow{\sim} U^{[r]}(G) \otimes U(\mathfrak{g}), \qquad x \otimes_D y \mapsto \sum xy_{(1)} \otimes \overline{y_{(2)}}.$$

Note that in this expression, $\overline{y_{(2)}}$ is the image of $y_{(2)} \in U^{[r]}(G)$ under the projection $\Upsilon_{r,r} : U^{[r]}(G) \twoheadrightarrow U(\mathfrak{g})$, where $\Upsilon_{r,r} : U^{[r]}(G) \twoheadrightarrow U(\mathfrak{g})$ is as defined in Subsection 3.2.2. By Remark 1.1(4) in [Schneider, 1990], the inverse of the map can *sends*

$$x \otimes \overline{y} \mapsto \sum xS(y_{(1)}) \otimes y_{(2)},$$

so

$$J'(h)(1 \otimes z) = \sum S(h_{(1)}) \otimes q(h_{(2)} \otimes z).$$

Now fix a $U(\mathfrak{g})$-comodule map $\gamma : U(\mathfrak{g}) \to U^{[r]}(G)$ such that $\Upsilon_{r,r} \circ \gamma = \mathrm{Id}_{U(\mathfrak{g})}$ and $S \circ \gamma = \gamma \circ S$. The proof of Proposition 3.3.1.7 illustrates a way to do this. We hence describe the isomorphism $J := J'S : U(\mathfrak{g}) \to E$ as follows:

$$x \mapsto (1 \otimes_D z \mapsto \sum \gamma(x)_{(1)} \otimes_D q(S(\gamma(x)_{(2)}) \otimes z)$$

for $x \in U(\mathfrak{g})$ and $z \in P$.

In particular, this remark shows that the action of $U(\mathfrak{g})$ on $\mathrm{Hom}_{G_r}(P, M)$ through the quotient $U^{[r]}(G)/U^{[r]}(G)\mathrm{Dist}^+(G_r)$ and the action of E on $\mathrm{Hom}_{G_r}(P, M)$ described above are compatible with the isomorphism in Lemma 4.1.1.4. So we get another way of seeing that an irreducible $U^{[r]}(G)$-module can be decomposed into an irreducible $\mathrm{Dist}(G_r)$-module and a $U(\mathfrak{g})$-module.

What is the benefit of this latter method of proof? Essentially, the initial approach uses the Hopf algebra structure of $U^{[r]}(G)$ to give certain vector spaces a module structure, while the latter approach uses the Hopf algebra structure to get an isomorphism $U(\mathfrak{g}) \cong E$ and then uses just the *algebra* structures to define the modules. Once one knows such an isomorphism exists, it is often-times easier in practice to work with an action which only depends on the algebra structure rather than an action which depends on the whole Hopf algebra structure.

For example, the second approach means that given a left $U(\mathfrak{g})$-module U and left $\mathrm{Dist}(G_r)$-module P, the equation

$$P \otimes_{\mathbb{K}} U \cong (U^{[r]}(G) \otimes_{\mathrm{Dist}(G_r)} P) \otimes_E U$$

allows us to write the $U^{[r]}(G)$-action down very easily. This will have particular use when considering the action of central elements of $U^{[r]}(G)$, such as elements of the form $\delta^{\otimes p} - \delta^p$. Furthermore, the action on E on $\mathrm{Hom}_{G_r}(P, M)$ is often easier to calculate with than the action of $U(\mathfrak{g})$ on the same.

4.1.2 Steinberg decomposition

Having now seen, through two different techniques, that an irreducible $U^{[r]}(G)$-module can be decomposed into a $\mathrm{Dist}(G_r)$-module and a $U(\mathfrak{g})$-module, there are two natural questions which follow. Firstly, how does this decomposition behave when one considers the reduced $U_\chi^{[r]}(G)$ instead of $U^{[r]}(G)$? And secondly, can we reverse this procedure? How well does the decomposition process characterise irreducible $U^{[r]}(G)$-modules?

We answer the first question first. As always throughout this chapter, G is a reductive algebraic group over an algebraically closed field $\mathbb{K}$ of positive characteristic p, and we make Assumption (R).

Proposition 4.1.2.1. *Let $\chi \in \mathfrak{g}^*$. If M is an irreducible $U_\chi^{[r]}(G)$-module and P is an irreducible $\mathrm{Dist}(G_r)$-module such that $M \cong P \otimes \mathrm{Hom}_{G_r}(P, M)$ as $U^{[r]}(G)$-modules, then $\mathrm{Hom}_{G_r}(P, M)$ is an irreducible $U_\chi(\mathfrak{g})$-module.*

Proof. From Remark 9 and Lemma 4.1.1.4, we know that $\mathrm{Hom}_{G_r}(P, M)$ is a $U(\mathfrak{g})$-module. Hence, all that remains is to show that for $x \in \mathfrak{g}$, the central element $x^p - x^{[p]}$ acts on $\mathrm{Hom}_{G_r}(P, M)$ as $\chi(x)^p$. Given $\delta \in \mathrm{Dist}^+_{p^r}(G)$, we know that $\delta^{\otimes p} - \delta^p$ is central in $U^{[r]}(G)$. Hence, the map

$$\rho(\delta^{\otimes p} - \delta^p) : U^{[r]}(G) \otimes_D P \to U^{[r]}(G) \otimes_D P$$

given by left multiplication by $\delta^{\otimes p} - \delta^p$ is a $U^{[r]}(G)$-module endomorphism, and so lies inside E. However, as we know that M is a $U_\chi^{[r]}(G)$-module, $\rho(\delta^{\otimes p} - \delta^p) \in E$ acts on $\mathrm{Hom}_{G_r}(P, M)$ as multiplication by $\chi(\delta)^p$.

Hence, we just need to show that, for $\alpha \in \Phi$, the element $\mathbf{e}_\alpha^p$ maps to $\rho((\mathbf{e}_\alpha^{(p^r)})^{\otimes p})$ and, for $1 \leqslant t \leqslant d$, the element $\mathbf{h}_t^p - \mathbf{h}_t$ maps to $\rho(\binom{\mathbf{h}_t}{p^r}^{\otimes p} - \binom{\mathbf{h}_t}{p^r})$ under the isomorphism $U(\mathfrak{g}) \cong E$.

This isomorphism is described in Remark 11. In particular, we know that

$$\mathbf{e}_\alpha^p = \overline{(\mathbf{e}_\alpha^{(p^r)})^{\otimes p}} \qquad \text{and} \qquad \mathbf{h}_t^p - \mathbf{h}_t = \overline{\binom{\mathbf{h}_t}{p^r}^{\otimes p} - \binom{\mathbf{h}_t}{p^r}}$$

for $\alpha \in \Phi$ and $1 \leqslant t \leqslant d$.

Observe that

$$\begin{aligned}\Delta((\mathbf{e}_\alpha^{(p^r)})^{\otimes p}) = \Delta(\mathbf{e}_\alpha^{(p^r)})^{\otimes p} &= \sum_{i=0}^{p^r} (\mathbf{e}_\alpha^{(i)})^{\otimes p} \otimes (\mathbf{e}_\alpha^{(p^r - i)})^{\otimes p} \\ &= (\mathbf{e}_\alpha^{(p^r)})^{\otimes p} \otimes 1 + 1 \otimes (\mathbf{e}_\alpha^{(p^r)})^{\otimes p},\end{aligned}$$

since $(\mathbf{e}_\alpha^{(i)})^{\otimes p} = 0$ for all $0 < i < p^r$, while

$$
\begin{aligned}
\Delta\left(\binom{\mathbf{h}_t}{p^r}^{\otimes p} - \binom{\mathbf{h}_t}{p^r}\right) &= \Delta\left(\binom{\mathbf{h}_t}{p^r}\right)^{\otimes p} - \Delta\left(\binom{\mathbf{h}_t}{p^r}\right) \\
&= \sum_{i=0}^{p^r} \binom{\mathbf{h}_t}{i}^{\otimes p} \otimes \binom{\mathbf{h}_t}{p^r - i}^{\otimes p} - \sum_{i=0}^{p^r} \binom{\mathbf{h}_t}{i} \otimes \binom{\mathbf{h}_t}{p^r - i} \\
&= \left(\binom{\mathbf{h}_t}{p^r}^{\otimes p} - \binom{\mathbf{h}_t}{p^r}\right) \otimes 1 + 1 \otimes \left(\binom{\mathbf{h}_t}{p^r}^{\otimes p} - \binom{\mathbf{h}_t}{p^r}\right)
\end{aligned}
$$

since $\binom{\mathbf{h}_t}{i}^{\otimes p} = \binom{\mathbf{h}_t}{i}$ for all $0 < i < p^r$.

Hence, $J'(\mathbf{e}_\alpha^p)(1 \otimes z) = 1 \otimes q((\mathbf{e}_\alpha^{(p^r)})^{\otimes p} \otimes z) - (\mathbf{e}_\alpha^{(p^r)})^{\otimes p} \otimes q(1 \otimes z)$. However, the $U^{[r]}(G)$-module structure on P comes through the map $U^{[r]}(G) \twoheadrightarrow \mathrm{Dist}(G_{r+1})$, so $q((\mathbf{e}_\alpha^{(p^r)})^{\otimes p} \otimes z) = 0$. Thus, $J'(\mathbf{e}_\alpha^p)(1 \otimes z) = -(\mathbf{e}_\alpha^{(p^r)})^{\otimes p} \otimes z$. Similarly, $J'(\mathbf{h}_t^p - \mathbf{h}_t)(1 \otimes z) = -(\binom{\mathbf{h}_t}{p^r}^{\otimes p} - \binom{\mathbf{h}_t}{p^r}) \otimes z$.

By Remark 3.8 in [Schneider, 1990], the algebra homomorphism $J : U(\mathfrak{g}) \to E$ is defined as $J = J'S$. Hence, we conclude that $J(\mathbf{e}_\alpha^p) = \rho((\mathbf{e}_\alpha^{(p^r)})^{\otimes p})$ for $\alpha \in \Phi$, and $J(\mathbf{h}_t^p - \mathbf{h}_t) = \rho(\binom{\mathbf{h}_t}{p^r}^{\otimes p} - \binom{\mathbf{h}_t}{p^r})$ for $1 \leqslant t \leqslant d$. The result follows. □

Corollary 4.1.2.2. *Suppose that G is connected and that $\mathfrak{g}$ and p are such that Premet's theorem holds.*[87] *Let M be an irreducible $U_\chi^{[r]}(G)$-module and P an irreducible* $\mathrm{Dist}(G_r)$*-module such that $M \cong P \otimes \mathrm{Hom}_{G_r}(P, M)$ as $U^{[r]}(G)$-modules. Then $p^{\dim(G\cdot\chi)/2}$ divides* $\dim \mathrm{Hom}_{G_r}(P, M)$.

To answer the remaining questions, we fix an irreducible $\mathrm{Dist}(G_r)$-module P. We define Γ_P to be the category of irreducible left $U^{[r]}(G)$-modules which decompose as $\mathrm{Dist}(G_r)$-modules into a direct sum of copies of ($\mathrm{Dist}(G_r)$-modules isomorphic to) P. This is a full subcategory of the category of irreducible left $U^{[r]}(G)$-modules. Furthermore, recall the notation of $\mathrm{mod}(U(\mathfrak{g}))$ for the category of finite-dimensional left $U(\mathfrak{g})$-modules.[88]

We examine the functor

$$
\Psi_P : \Gamma_P \to \mathrm{mod}(E) = \mathrm{mod}(U(\mathfrak{g}))
$$

which sends $M \in \Gamma_P$ to $\mathrm{Hom}_{G_r}(P, M)$. The following theorem should be compared with Theorem 3.1 in [Witherspoon, 1999].

Theorem 4.1.2.3. *There is an equivalence of categories between Γ_P and $\mathrm{Irr}(E)$. In particular, this equivalence is obtained from the maps*

$$
\Psi_P : \Gamma_P \to \mathrm{Irr}(E), \qquad \Psi_P(M) = \mathrm{Hom}_{G_r}(P, M);
$$

$$
\Phi_P : \mathrm{Irr}(E) \to \Gamma_P, \qquad \Phi_P(N) = P \otimes_{\mathbb{K}} N.
$$

[87] See Theorem 2.4.3.2 in Subsection 2.4.3.

[88] Recall that every irreducible $U(\mathfrak{g})$-module has finite dimension, so the category of irreducible left $U(\mathfrak{g})$-modules, $\mathrm{Irr}(U(\mathfrak{g}))$, is a full subcategory of $\mathrm{mod}(U(\mathfrak{g}))$.

Proof. We maintain the convention $D = \mathrm{Dist}(G_r)$ to make formulas clearer.

If $M \in \Gamma_P$, then Lemma 4.1.1.2, Remark 9 and Theorem 4.1.1.3 show that

$$\Psi_P(M) = \mathrm{Hom}_{G_r}(P, M) = \mathrm{Hom}_{U^{[r]}(G)}(U^{[r]}(G) \otimes_D P, M)$$

is a left E-module; that $P \otimes_{\mathbb{K}} \Psi_P(M)$ is a left $U^{[r]}(G)$-module; that $P \otimes_{\mathbb{K}} \Psi_P(M)$ is isomorphic to $(U^{[r]}(G) \otimes_D P) \otimes_E \Psi_P(M)$ as $U^{[r]}(G)$-modules; and that

$$\eta_M : (U^{[r]}(G) \otimes_D P) \otimes_E \Psi_P(M) \to M, \qquad \eta_M(a \otimes_D z \otimes_E \phi) = \phi(a \otimes_D z)$$

is an isomorphism of $U^{[r]}(G)$-modules.

Note that $\Psi_P(M)$ is an irreducible E-module, since if $\Psi_P(M)$ contains a proper non-trivial submodule U then

$$P \otimes_{\mathbb{K}} U \cong (U^{[r]}(G) \otimes_D P) \otimes_E U$$

is a proper non-trivial $U^{[r]}(G)$-submodule of the irreducible $U^{[r]}(G)$-module

$$M \cong (U^{[r]}(G) \otimes_D P) \otimes_E \Psi_P(M) \cong P \otimes_{\mathbb{K}} \Psi_P(M).$$

Now, suppose N is an irreducible left E-module. It is proved in Lemma 4.1.1.2 that

$$\Phi_P(N) := P \otimes_{\mathbb{K}} N \cong (U^{[r]}(G) \otimes_D P) \otimes_E N$$

is a left $U^{[r]}(G)$-module, and furthermore that the structure is such that $\Phi_P(N)$ is a direct sum of copies of P as a $\mathrm{Dist}(G_r)$-module.

We now wish to show that $\mathrm{Hom}_D(P, \Phi_P(N)) \cong N$ as left E-modules. Define

$$\sigma_N : N \to \mathrm{Hom}_D(P, \Phi_P(N)) \quad \text{by} \quad \sigma_N(n)(z) = z \otimes n \in P \otimes_{\mathbb{K}} N.$$

Since

$$\mathrm{Hom}_D(P, \Phi_P(N)) \cong \mathrm{Hom}_{U^{[r]}(G)}(U^{[r]}(G) \otimes_D P, \Phi_P(N))$$

as left E-modules and

$$P \otimes_{\mathbb{K}} N \cong (U^{[r]}(G) \otimes_D P) \otimes_E N$$

as left $U^{[r]}(G)$-modules, we can also write this map as

$$\sigma_N : N \to \mathrm{Hom}_{U^{[r]}(G)}(U^{[r]}(G) \otimes_D P, (U^{[r]}(G) \otimes_D P) \otimes_E N),$$

$$\sigma_N(n)(a \otimes_D z) = (a \otimes_D z) \otimes_E n$$

for $n \in N$, $z \in P$ and $a \in U^{[r]}(G)$.

It is straightforward to see that $\sigma_N(n)$ is a $U^{[r]}(G)$-module homomorphism from $U^{[r]}(G) \otimes_D P$ to $(U^{[r]}(G) \otimes_D P) \otimes_E N$, and also that σ_N is a linear map. We show that σ_N is E-linear. It is enough to show that for $f \in E$, $n \in N$, $z \in P$ and $a \in U^{[r]}(G)$, we have that

$$(f \cdot \sigma_N(n))(a \otimes_D z) = \sigma_N(f \cdot n)(a \otimes_D z).$$

Note that

$$(f \cdot \sigma_N(n))(a \otimes_D z) = \sigma_N(n)(f(a \otimes_D z)) = f(a \otimes_D z) \otimes_E n,$$

while

$$\sigma_N(f \cdot n)(a \otimes_D z) = (a \otimes_D z) \otimes_E (f \cdot n).$$

Since the right E-module structure on $U^{[r]}(G) \otimes_D P$ comes from the evaluation map, the result holds from the definition of the tensor product.

Hence, σ_N is an E-module homomorphism. It is clear that σ_N is injective from the description $\sigma_N(n)(z) = z \otimes n \in P \otimes_{\mathbb{K}} N$ for $n \in N$, $z \in P$. Furthermore, by above,

$$\Phi_P(N) \cong \bigoplus_{i=1}^{k} P$$

as $\mathrm{Dist}(G_r)$-modules. Now, $k = \dim(N)$ as $\dim(\Phi_P(N)) = \dim(P)\dim(N)$ and $\dim\left(\bigoplus_{i=1}^{k} P\right) = k\dim(P)$. Hence,

$$\mathrm{Hom}_{G_r}(P, \Phi_P(N)) \cong \mathrm{Hom}_{G_r}\left(P, \bigoplus_{i=1}^{k} P\right) = \mathbb{K}^k,$$

since $\mathrm{Hom}_{G_r}(P, P) = \mathbb{K}$. Thus, $\dim(N) = k = \dim(\mathrm{Hom}_{G_r}(P, \Phi_P(N)))$. Together with the injectivity, this proves that σ_N is an isomorphism of E-modules.

Furthermore, $\Phi_P(N)$ is an irreducible $U^{[r]}(G)$-module since if it contains a proper non-trivial submodule L then

$$\mathrm{Hom}_{G_r}(P, L) \cong \mathrm{Hom}_{U^{[r]}(G)}(U^{[r]}(G) \otimes_D P, L)$$

is a proper non-trivial E-submodule of

$$N \cong \mathrm{Hom}_{U^{[r]}(G)}(U^{[r]}(G) \otimes_D P, \Phi_P(N)) \cong \mathrm{Hom}_D(P, \Phi_P(N)),$$

contradicting the irreducibility of N.

In conclusion, we have shown that the maps Ψ_P and Φ_P are well-defined; that for any irreducible $U^{[r]}(G)$-module M, we have $\Phi_P(\Psi_P(M)) \cong M$ as $U^{[r]}(G)$-modules; and that for any irreducible E-module N, we have $\Psi_P(\Phi_P(N)) \cong N$ as E-modules. It is then straightforward to see that this bijection is in fact an equivalence of categories. □

Remark 12. *This proof, in fact, shows that for any E-module N, not necessarily* *irreducible, it is true that*

$$N \cong \mathrm{Hom}_{G_r}(P, P \otimes_{\mathbb{K}} N) = \mathrm{Hom}_{G_r}(P, (U^{[r]}(G) \otimes_D P) \otimes_E N)$$

as E-modules.

For each $\mathbb{K}$-algebra R we consider in this chapter, we denote by $\underline{\mathrm{Irr}}(R)$ the set of isomorphism classes of irreducible R-modules.

Corollary 4.1.2.4. *There is a bijection*

$$\Psi : \underline{\mathrm{Irr}}(U^{[r]}(G)) \to \underline{\mathrm{Irr}}(\mathrm{Dist}(G_r)) \times \underline{\mathrm{Irr}}(U(\mathfrak{g}))$$

which sends M to $(P, \mathrm{Hom}_{G_r}(P, M))$, where P is the unique (up to isomorphism) irreducible $\mathrm{Dist}(G_r)$-submodule of M. Furthermore, the reverse map sends (P, N) to the $U^{[r]}(G)$-module $(U^{[r]}(G) \otimes_D P) \otimes_{U(\mathfrak{g})} N = P \otimes_{\mathbb{K}} N$.

We furthermore see that this process also behaves nicely when one passes to reduced enveloping algebras.

Lemma 4.1.2.5. *Let $P \in \mathrm{Irr}(\mathrm{Dist}(G_r))$ and $N \in \mathrm{Irr}(U(\mathfrak{g}))$ with p-character $\chi \in \mathfrak{g}^*$ (so $N \in \mathrm{Irr}(U_\chi(\mathfrak{g}))$). Then the following results hold.*

1. *The left $U^{[r]}(G)$-module $(U^{[r]}(G) \otimes_D P) \otimes_{U(\mathfrak{g})} N$ is a left $U_\chi^{[r]}(G)$-module.*
2. *$U_\chi^{[r]}(G) \otimes_D P$ is a right $U_\chi(\mathfrak{g})$-module.*
3. *As $U_\chi^{[r]}(G)$-modules,*

$$(U^{[r]}(G) \otimes_D P) \otimes_{U(\mathfrak{g})} N \cong (U_\chi^{[r]}(G) \otimes_D P) \otimes_{U_\chi(\mathfrak{g})} N.$$

Proof. (1) To show that $(U^{[r]}(G) \otimes_D P) \otimes_{U(\mathfrak{g})} N$ is a left $U_\chi^{[r]}(G)$-module, it is enough to show that $\delta^{\otimes p} - \delta^p - \chi(\delta)^p$ acts on it by zero multiplication for all $\delta \in \mathrm{Dist}^+_{p^r}(G)$. Set $\delta \in \mathrm{Dist}^+_{p^r}(G)$, and let $x = \Upsilon_{r,r}(\delta) \in \mathfrak{g}$.

Let $u \in U^{[r]}(G)$, $z \in P$ and $n \in N$. Then

$$\begin{aligned}(\delta^{\otimes p} - \delta^p - \chi(\delta)^p) \cdot (u \otimes_D z) \otimes_{U(\mathfrak{g})} n &= (u \otimes_D z) \cdot (x^p - x^{[p]} - \chi(x)^p) \otimes_{U(\mathfrak{g})} n \\ &= (u \otimes_D z) \otimes_{U(\mathfrak{g})} (x^p - x^{[p]} - \chi(x)^p) \cdot n \\ &= 0.\end{aligned}$$

(2) To show that $U_\chi^{[r]}(G) \otimes_D P$ is a right $U_\chi(\mathfrak{g})$-module, first note that $\mathrm{Dist}(G_r)$ is a subalgebra of $U_\chi^{[r]}(G)$, so the tensor product makes sense. We will show that $U_\chi^{[r]}(G) \otimes_D P$ is a right E-module, on which the left multiplication by $\delta^{\otimes p} - \delta^p - \chi(\delta)^p$ is zero for all $\delta \in \mathrm{Dist}^+_{p^r}(G)$.

Let $f \in \mathrm{End}_{U^{[r]}(G)}(U^{[r]}(G) \otimes_D P)^{op}$. We want a linear map $\widetilde{T_f} : U_\chi^{[r]}(G) \otimes_D P \to U_\chi^{[r]}(G) \otimes_D P$. By the universal property of the tensor product, it is enough to give a linear map $T_f : U_\chi^{[r]}(G) \times P \to U^{[r]}(G) \otimes_D P$ which is $\mathrm{Dist}(G_r)$-balanced.

Define $T_f(\overline{u}, z) = \overline{f(u \otimes_D z)}$ for $u \in U^{[r]}(G)$ and $z \in P$, where $\overline{f(u \otimes_D z)}$ is the image of $f(u \otimes_D z)$ under the map $U^{[r]}(G) \otimes_D P \twoheadrightarrow U_\chi^{[r]}(G) \otimes_D P$. First, we must see that this is well-defined. Suppose $\overline{u} = \overline{v} \in U_\chi^{[r]}(G)$. Hence, $u - v \in I \trianglelefteq U^{[r]}(G)$, where I is the ideal generated by $\delta^{\otimes p} - \delta^p - \chi(\delta)^p$ for $\delta \in \mathrm{Dist}_{p^r}^+(G)$. So $f((u-v) \otimes_D z) \in I \otimes_D P$, so $\overline{f((u-v) \otimes_D z)} = 0$. Furthermore, for $d \in \mathrm{Dist}(G_r)$, we have

$$T_f(\overline{u} \cdot d, z) = T_f(\overline{ud}, z) = \overline{f(ud \otimes_D z)} = \overline{f(u \otimes_D dz)} = T_f(\overline{u}, d \cdot z).$$

Hence, we obtain a linear map $\widetilde{T_f} : U_\chi^{[r]}(G) \otimes_D P \to U_\chi^{[r]}(G) \otimes_D P$. It is straightforward to see that $\widetilde{T_f}\widetilde{T_g} = \widetilde{T_{fg}}$, so $U_\chi^{[r]}(G) \otimes_D P$ is a right E-module. One may then check that the action of left multiplication by $\delta^{\otimes p} - \delta^p - \chi(\delta)^p$ is zero for all $\delta \in \mathrm{Dist}_{p^r}^+(G)$.

Hence $U_\chi^{[r]}(G) \otimes_D P$ is a right $U_\chi(\mathfrak{g})$-module.

(3) All that remains is to show the isomorphism $(U^{[r]}(G) \otimes_D P) \otimes_{U(\mathfrak{g})} N \cong (U_\chi^{[r]}(G) \otimes_D P) \otimes_{U_\chi(\mathfrak{g})} N$.

Define the map

$$F : (U^{[r]}(G) \otimes_D P) \times N \to (U_\chi^{[r]}(G) \otimes_D P) \otimes_{U_\chi(\mathfrak{g})} N$$

by sending the elements $(u \otimes_D z, n)$ to $(\overline{u} \otimes_D z) \otimes_{U_\chi(\mathfrak{g})} n$, where $\overline{u} = u + I$. It is easy to see that is map is a well-defined $U_\chi^{[r]}(G)$-module homomorphism. It is also $U(\mathfrak{g})$-balanced:

$$F((u \otimes_D z) \cdot f, n) = \overline{f(u \otimes_D z)} \otimes_{U_\chi(\mathfrak{g})} n = (u \otimes_D z) \otimes_{U_\chi(\mathfrak{g})} \overline{f} \cdot n = F(u \otimes_D z, f \cdot n),$$

where $u \in U^{[r]}(G)$, $z \in P$, $n \in N$, $f \in E \cong U(\mathfrak{g})$ and $\overline{f} = f + J \in E/J$, where J is the ideal in E generated by left multiplications by the elements $\delta^{\otimes p} - \delta^p - \chi(\delta)^p$ for $\delta \in \mathrm{Dist}_{p^r}^+(G)$. Hence, there is a $U_\chi^{[r]}(G)$-module homomorphism $\widetilde{F} : (U^{[r]}(G) \otimes_D P) \otimes_{U(\mathfrak{g})} N \to (U_\chi^{[r]}(G) \otimes_D P) \otimes_{U_\chi(\mathfrak{g})} N$.

Furthermore, we define

$$H : (U_\chi^{[r]}(G) \otimes_D P) \times N \to (U^{[r]}(G) \otimes_D P) \otimes_{U(\mathfrak{g})} N$$

by sending the elements $(\overline{u} \otimes_D z, n)$ to $(u \otimes_D z) \otimes_{U(\mathfrak{g})} n$. This map is well-defined, since $(U^{[r]}(G) \otimes_D P) \otimes_{U(\mathfrak{g})} N$ is a $U_\chi^{[r]}(G)$-module, and a homomorphism of $U_\chi^{[r]}(G)$-modules. It is also $U_\chi(\mathfrak{g})$-balanced:

$$H((\overline{u} \otimes_D z) \cdot \overline{f}, n) = f(u \otimes_D z) \otimes_{U_\chi(\mathfrak{g})} n = (u \otimes_D z) \otimes_{U_\chi(\mathfrak{g})} f \cdot n = F((u \otimes_D z), \overline{f} \cdot n),$$

where $u \in U^{[r]}(G)$, $z \in P$, $n \in N$, $f \in E \cong U(\mathfrak{g})$ and $\overline{f} = f + J \in E/J$. This gives a $U_\chi^{[r]}(G)$-module homomorphism $\widetilde{H} : (U_\chi^{[r]}(G) \otimes_D P) \otimes_{U_\chi(\mathfrak{g})} N \to (U^{[r]}(G) \otimes_D P) \otimes_{U(\mathfrak{g})} N$.

It is straightforward to see that $\widetilde{F}$ and $\widetilde{H}$ are inverse to each other. The result follows. $\square$

This proof shows the benefit of working with the algebra E, which we know is isomorphic to $U(\mathfrak{g})$, rather than working directly with $U(\mathfrak{g})$. In particular, we did not need to use anything other than basic properties of associative algebras to prove the results.

Corollary 4.1.2.6. *There is a bijection*

$$\Psi_\chi : \underline{\mathrm{Irr}}(U_\chi^{[r]}(G)) \to \underline{\mathrm{Irr}}(\mathrm{Dist}(G_r)) \times \underline{\mathrm{Irr}}(U_\chi(\mathfrak{g}))$$

which sends M to $(P, \mathrm{Hom}_{G_r}(P, M))$, where P is the unique (up to isomorphism) irreducible $\mathrm{Dist}(G_r)$-submodule of M. The inverse map sends (P, N) to $(U_\chi^{[r]}(G) \otimes_{\mathrm{Dist}(G_r)} P) \otimes_{U_\chi(\mathfrak{g})} N \cong P \otimes_{\mathbb{K}} N$.

4.1.3 Teenage Verma modules

We can use the previous subsection to deduce some structural results about irreducible $U_\chi^{[r]}(G)$-modules. We start by defining the following vector subspace of $U^{[r]}(G)$, using the $[\![\cdot]\!]$ notation from Subsection 3.3.2:

$$\widehat{U^{[r]}(B)} := \mathbb{K} - \mathrm{span}\left\{ \prod_{\alpha\in\Phi^+} \mathbf{e}_\alpha^{[\![i_\alpha]\!]} \prod_{t=1}^{d} \binom{\mathbf{h}_t}{[\![k_t]\!]} \prod_{\alpha\in\Phi^+} \mathbf{e}_{-\alpha}^{[\![j_\alpha]\!]} : 0 \leqslant i_\alpha, k_t,\ 0 \leqslant j_\alpha < p^r \right\}.$$

This vector space is, in fact, a subalgebra of $U^{[r]}(G)$ by the commutation equations given in Lecture 15 in [Steinberg, 1968]. Furthermore, the Hopf algebra structure on $U^{[r]}(G)$ makes $\widehat{U^{[r]}(B)}$ into a Hopf subalgebra of $U^{[r]}(G)$.

Clearly $\mathrm{Dist}(G_r)$ is a subalgebra of $\widehat{U^{[r]}(B)}$, it is normal since it is normal in $U^{[r]}(G)$, and $\widehat{U^{[r]}(B)}$ is free as both a left and right $\mathrm{Dist}(G_r)$-module. From Subsection 3.2.2, we know that the map $\Upsilon_{r,r} : U^{[r]}(G) \to U(\mathfrak{g})$ is a surjective Hopf algebra homomorphism. It is easy to see from the bases that this map restricts to a surjective Hopf algebra homomorphism $\widehat{U^{[r]}(B)} \twoheadrightarrow U(\mathfrak{b})$, with kernel $\widehat{U^{[r]}(B)}\mathrm{Dist}^+(G_r) = \mathrm{Dist}^+(G_r)\widehat{U^{[r]}(B)}$. In particular, $\mathrm{Dist}(G_r) \subseteq \widehat{U^{[r]}(B)}$ is a $U(\mathfrak{b})$-module extension, with $\mathrm{Dist}(G_r) = \widehat{U^{[r]}(B)}^{coU(\mathfrak{b})}$.

Lemma 4.1.3.1. *Let $P \in \mathrm{Irr}(\mathrm{Dist}(G_r))$. Then $\mathrm{End}_{\widehat{U^{[r]}(B)}}(\widehat{U^{[r]}(B)} \otimes_D P) \cong U(\mathfrak{b})$.*

Proof. This follows as in Lemma 4.1.1.4, since $\widehat{U^{[r]}(B)}$ is a subalgebra of $U^{[r]}(G)$. $\square$

It is straightforward to see that the proof of Theorem 4.1.1.1 and the proof of Theorem 4.1.2.3, *supra*, hold similarly in this context. In other words, we have the following proposition.

Proposition 4.1.3.2. *There is a bijection*

$$\widehat{\Psi} : \underline{\mathrm{Irr}}(\widehat{U^{[r]}(B)}) \xrightarrow{\sim} \underline{\mathrm{Irr}}(\mathrm{Dist}(G_r)) \times \underline{\mathrm{Irr}}(U(\mathfrak{b}))$$

which sends M to $(P, \mathrm{Hom}_{G_r}(P, M))$, where P is the unique (up to isomorphism) irreducible $\mathrm{Dist}(G_r)$*-submodule of M. The inverse map sends (P, N) to the $\widehat{U^{[r]}(B)}$-module $(\widehat{U^{[r]}(B)} \otimes_D P) \otimes_{U(\mathfrak{b})} N = P \otimes_{\mathbb{K}} N$.*

Applying Proposition 4.1.2.1 and Lemma 4.1.2.5 in this context, we get the following corollary.

Corollary 4.1.3.3. *For $\chi \in \mathfrak{b}^*$, the bijection in Proposition 4.1.3.2 restricts to a bijection*

$$\widehat{\Psi_\chi} : \underline{\mathrm{Irr}}(\widehat{U_\chi^{[r]}(B)}) \xrightarrow{\sim} \underline{\mathrm{Irr}}(\mathrm{Dist}(G_r)) \times \underline{\mathrm{Irr}}(U_\chi(\mathfrak{b})).$$

Assume from now on that $\chi(\mathfrak{n}^+) = 0$. We see in Subsection 2.4.3 that, if $N \in \mathrm{Irr}(U_\chi(\mathfrak{b}))$, then $N = \mathbb{K}_\lambda$ for some $\lambda \in \Lambda_\chi$, where $\mathbb{K}_\lambda$ denotes the 1-dimensional $\mathfrak{b}$-module on which $\mathfrak{n}^+$ acts trivially and $h \in \mathfrak{h}$ acts through multiplication by $\lambda(h)$. Recall here that

$$\Lambda_\chi := \{\lambda \in \mathfrak{h}^* \mid \lambda(h)^p - \lambda(h) = \chi(h)^p \text{ for all } h \in \mathfrak{h}\}.$$

Hence, there is a bijection,

$$\widehat{\Psi} : \underline{\mathrm{Irr}}(\widehat{U_\chi^{[r]}(B)}) \xrightarrow{\sim} \underline{\mathrm{Irr}}(\mathrm{Dist}(G_r)) \times \Lambda_\chi.$$

In other words, every irreducible $\mathrm{Dist}(G_r)$-module P can be extended to an irreducible $\widehat{U_\chi^{[r]}(B)}$-module, and there is (up to isomorphism) one such way to do this for each $\lambda \in \Lambda_\chi$. For each $\lambda \in \Lambda_\chi$, we can hence define the $U_\chi^{[r]}(G)$-module

$$\begin{aligned}
U_\chi^{[r]}(G) \otimes_{\widehat{U_\chi^{[r]}(B)}} (P \otimes_{\mathbb{K}} \mathbb{K}_\lambda) &= U_\chi^{[r]}(G) \otimes_{\widehat{U_\chi^{[r]}(B)}} (\widehat{U_\chi^{[r]}(B)} \otimes_D P) \otimes_{U_\chi(\mathfrak{b})} \mathbb{K}_\lambda \\
&\overset{\star}{=} (U_\chi^{[r]}(G) \otimes_{\widehat{U_\chi^{[r]}(B)}} \widehat{U_\chi^{[r]}(B)} \otimes_D P) \otimes_{U_\chi(\mathfrak{b})} \mathbb{K}_\lambda \\
&= (U_\chi^{[r]}(G) \otimes_D P) \otimes_{U_\chi(\mathfrak{b})} \mathbb{K}_\lambda \\
&= (U_\chi^{[r]}(G) \otimes_D P) \otimes_{U_\chi(\mathfrak{g})} U_\chi(\mathfrak{g}) \otimes_{U_\chi(\mathfrak{b})} \mathbb{K}_\lambda \\
&= (U_\chi^{[r]}(G) \otimes_D P) \otimes_{U_\chi(\mathfrak{g})} Z_\chi(\lambda) \\
&= P \otimes_{\mathbb{K}} Z_\chi(\lambda).
\end{aligned}$$

Here, equality $(\star)$ follows from an easy check.

We call this $U_\chi^{[r]}(G)$-module the **teenage Verma module** $Z_\chi^r(P, \lambda)$. Note that $\dim(Z_\chi^r(P, \lambda)) = p^{\dim(\mathfrak{n}^-)} \dim(P)$. Frobenius reciprocity then gives the following proposition.

Proposition 4.1.3.4. *Every irreducible $U_\chi^{[r]}(G)$-module is a quotient of a teenage Verma module $Z_\chi^r(P, \lambda)$ for some $P \in \mathrm{Irr}(\mathrm{Dist}(G_r))$ and $\lambda \in \Lambda_\chi$.*

Despite the fact that baby Verma modules and teenage Verma modules need not be irreducible, the following lemma shows that the correspondence in Corollary 4.1.2.6 can be extended to these modules.

Lemma 4.1.3.5. *For $P \in \mathrm{Irr}(\mathrm{Dist}(G_r))$ and $\lambda \in \Lambda_\chi$, we have $\mathrm{Hom}_{G_r}(P, Z^r_\chi(P,\lambda)) \cong Z_\chi(\lambda)$ as left $U_\chi(\mathfrak{g})$-modules.*

Proof. This follows directly from Remark 12. □

We also obtain the following structural result.

Proposition 4.1.3.6. *Suppose $M \in \mathrm{Irr}(U^{[r]}_\chi(G))$, $P \in \mathrm{Irr}(\mathrm{Dist}(G_r))$ and $N \in \mathrm{Irr}(U_\chi(\mathfrak{g}))$ such that $\Psi_\chi(M) = (P, N)$. Then M is an irreducible quotient of $Z^r_\chi(P,\lambda)$ if and only if N is an irreducible quotient of $Z_\chi(\lambda)$.*

Proof. ($\Longrightarrow$) By definition of Ψ_χ and Lemma 4.1.3.5, $N = \mathrm{Hom}_{G_r}(P, M)$ and $Z_\chi(\lambda) = \mathrm{Hom}_{G_r}(P, Z^r_\chi(P,\lambda))$. Let $\pi : Z^r_\chi(P,\lambda) \to M$ be the given surjection. We then define the map $\eta : Z_\chi(\lambda) \to N$ by defining the map $\eta : \mathrm{Hom}_{G_r}(P, Z^r_\chi(P,\lambda)) \to \mathrm{Hom}_{G_r}(P, M)$ as $\eta(f)(z) = \pi f(z)$ for $f \in \mathrm{Hom}_{G_r}(P, Z^r_\chi(P,\lambda))$ and $z \in P$. It is straightforward to check that this is an E-module homomorphism, hence a $U(\mathfrak{g})$-module homomorphism, hence a $U_\chi(\mathfrak{g})$-module homomorphism. It is surjective as N is irreducible.

($\Longleftarrow$) By the definitions of Ψ_χ and $Z^r_\chi(P,\lambda)$, we have $M = (U^{[r]}_\chi(G) \otimes_D P) \otimes_{U_\chi(\mathfrak{g})} N$ and $Z^r_\chi(P,\lambda) = (U^{[r]}_\chi(G) \otimes_D P) \otimes_{U_\chi(\mathfrak{g})} Z_\chi(\lambda)$. The result then follows from the functoriality of the tensor product and the irreducibility of M. □

As an application, we can use teenage Verma modules to characterise (most) irreducible $U_\chi(SL_2)$-modules. A direct computation of these can also be found in [Westaway, 2018]; this is also a special case of Theorem 4.1.4.1, *infra.*

Theorem 4.1.3.7 (Classification of irreducible $U^{[r]}_\chi(SL_2)$-modules)**.** *If the characteristic of $\mathbb{K}$ is odd, we have the following classification of irreducible $U^{[r]}_\chi(SL_2)$-modules, for $(\chi \in \mathfrak{sl}_2^*)^{[r]}$:*

1. *If $\chi \neq 0$ is semisimple, then the irreducible modules are the $Z^r_\chi(P,\lambda)$ for P an irreducible $\mathrm{Dist}(SL_{2,r})$-module and $\lambda \in \Lambda_\chi$. Furthermore, these are all non-isomorphic, so there are exactly p^{r+1} non-isomorphic $U^r_\chi(SL_2)$-modules.*

2. *If $\chi \neq 0$ is nilpotent, then the irreducible modules are the $Z^r_\chi(P,\lambda)$ for P an irreducible $\mathrm{Dist}(SL_{2,r})$-module and $\lambda \in \Lambda_\chi = \mathbb{F}_p$. Furthermore, $Z^r_\chi(P,\lambda) = Z^{[r]}_\chi(P',\lambda')$ if and only if $P \cong P'$ and $\lambda = \lambda'$ or $\lambda' = p-\lambda-2$ and $\lambda \leqslant p-2$ (as an element of $\{0,1,\ldots,p-1\}$), so there are exactly $p^r(\frac{p+1}{2})$ non-isomorphic $U^{[r]}_\chi(SL_2)$-modules.*

3. *If $\chi = 0$, every irreducible $U^r_0(SL_2)$-module is the unique irreducible quotient of $Z^r_\chi(P,\lambda)$ for P an irreducible $\mathrm{Dist}(SL_{2,r})$-module and $\lambda \in \Lambda_0 = \mathbb{F}_p$.*

Proof. This follows from Corollary 4.1.2.6, the definition of the teenage Verma modules $Z^r(P,\lambda)$, and the classification of irreducible $\mathfrak{sl}_2$-modules in Theorem 2.4.3.3. □

4.1.4 Consequences

From now on, let us make the following assumptions:[89]

(H1) The derived group of G is simply-connected.

(H2) The prime p is good[90] for G.

(H3) There is a non-degenerate G-invariant bilinear form on $\mathfrak{g}$.

In particular, (H3) gives rise to an isomorphism of G-modules[91] $\mathfrak{g} \to \mathfrak{g}^*$. This allows us to transfer properties of elements of $\mathfrak{g}$ to properties of elements of $\mathfrak{g}^*$. For example, we say that $\chi \in \mathfrak{g}^*$ is **semisimple** if the corresponding element $x \in \mathfrak{g}$ is semisimple.[92] Similarly, we say that $\chi \in \mathfrak{g}^*$ is **nilpotent** if the corresponding element $x \in \mathfrak{g}$ is nilpotent.[93]

Furthermore, we say that $x \in \mathfrak{g}$ is **regular** if $\dim(C_G(x)) = \dim(\mathfrak{h})$, where $C_G(x) := \{g \in G \,|\, g{\cdot}x = x\}$. We hence say that $\chi \in \mathfrak{g}^*$ is **regular** if the corresponding $x \in \mathfrak{g}$ is regular - this is equivalent to the requirement that $\dim(C_G(\chi)) = \dim(\mathfrak{h})$, where $C_G(\chi) := \{g \in G \,|\, g \cdot \chi = \chi\}$.

With these definitions in mind, we get the following proposition.

Theorem 4.1.4.1. *Let M be an irreducible $U_\chi^{[r]}(G)$-module, for $\chi \in \mathfrak{g}^*$, and let P be the unique (up to isomorphism) irreducible $\mathrm{Dist}(G_r)$-submodule of M. The following results hold.*

(1) *There exists $\lambda \in \Lambda_\chi$ such that M is an irreducible quotient of $Z_\chi^r(P,\lambda)$.*

(2) *If χ is regular, then there exists $P \in \mathrm{Irr}(\mathrm{Dist}(G_r))$ and $\lambda \in \Lambda_\chi$ such that $M \cong Z_\chi^r(P,\lambda)$.*

(3) *If χ is regular semisimple, then $Z_\chi^r(P,\lambda) \cong Z_\chi^r(\widetilde{P},\mu)$ if and only if $P \cong \widetilde{P}$ and $\lambda = \mu$.*

(4) *If χ is regular nilpotent and $\chi(\mathbf{e}_{-\alpha}) \neq 0$ for all $\alpha \in \Pi$, then $Z_\chi^r(P,\lambda) \cong Z_\chi^r(\widetilde{P},\mu)$ if and only if $P \cong \widetilde{P}$ and $\lambda \in W \bullet \mu$, where W is the Weyl group of Φ and $\bullet$ represents the dot-action.*

Proof. (1) By above, there exists $Q \in \mathrm{Irr}(\mathrm{Dist}(G_r))$ and $\lambda \in \Lambda_\chi$ such that M is an irreducible quotient of $Z_\chi^r(Q,\lambda)$. Frobenius reciprocity then shows that

$$\mathrm{Hom}_{U_\chi^{[r]}(G)}(Z_\chi^r(Q,\lambda), M) \cong \mathrm{Hom}_{\widehat{U_\chi^{[r]}(B)}}(Q \otimes_{\mathbb{K}} \mathbb{K}_\lambda, M).$$

[89]See Chapter 6 in [Jantzen, 1997] for more details.

[90]Recall that a prime p being good for G is a property of the root system, and specifically means that: $p \neq 2$ for types B_n ($n \geqslant 2$), C_n ($n \geqslant 2$), or D_n ($n \neq 4$); $p \neq 2, 3$ for types E_6, E_7, F_4 or G_2; and $p \neq 2, 3, 5$ for type E_8.

[91]Recall that $\mathfrak{g}$ is a G-module via the adjoint action and $\mathfrak{g}^*$ is a G-module via the coadjoint action.

[92]In fact this is equivalent to the requirement that $g \cdot \chi(\mathfrak{n}^+ \oplus \mathfrak{n}^-) = 0$ for some $g \in G$, under the coadjoint action.

[93]This is equivalent to the requirement that $g \cdot \chi(\mathfrak{b}) = 0$ for some $g \in G$, under the coadjoint action.

In particular, as $M \neq 0$, the $\mathrm{Dist}(G_r)$-module $Q \subseteq Z^r_\chi(Q,\lambda)$ is not in the kernel of the surjection $\pi : Z^r_\chi(Q,\lambda) \twoheadrightarrow M$. Hence, the surjection restricts to a $\mathrm{Dist}(G_r)$-isomorphism $Q \to \pi(Q)$, so Q is an irreducible $\mathrm{Dist}(G_r)$-submodule of M. As a result, $Q \cong P$, and we can say that M is an irreducible quotient of $Z^r_\chi(P,\lambda)$ for some $\lambda \in \Lambda_\chi$.

(2) The bijection Ψ_χ sends M to the pair (P,N) for some $N \in \mathrm{Irr}(U_\chi(\mathfrak{g}))$, and $\dim(M) = \dim(P)\dim(N)$. Since χ is regular, $\dim(N) = p^{\dim(\mathfrak{n}^-)}$.

However, by (1), M is an irreducible quotient of $Z^r_\chi(P,\lambda)$ for some $\lambda \in \Lambda_\chi$. Furthermore, $\dim(Z^r_\chi(P,\lambda)) = p^{\dim(\mathfrak{n}^-)}\dim(P)$. Hence, $M \cong Z^r_\chi(P,\lambda)$.

(3) Suppose $Z^r_\chi(P,\lambda) \cong Z^r_\chi(\widetilde{P},\mu)$. The $U^{[r]}_\chi(G)$-module $Z^r_\chi(P,\lambda)$ is an irreducible module containing P, while $Z^r_\chi(\widetilde{P},\mu)$ is an irreducible $U^{[r]}_\chi(G)$-module containing $\widetilde{P}$. Since each irreducible $U^{[r]}_\chi(G)$-module contains a unique irreducible $\mathrm{Dist}(G_r)$-submodule, we obtain that P and $\widetilde{P}$ are isomorphic $\mathrm{Dist}(G_r)$-modules.

Hence,

$$\mathrm{Hom}_{G_r}(P, Z^r_\chi(P,\lambda)) \cong \mathrm{Hom}_{G_r}(\widetilde{P}, Z^r_\chi(\widetilde{P},\mu)),$$

and so

$$Z_\chi(\lambda) \cong Z_\chi(\mu).$$

By [Jantzen, 2004, B.10], $\lambda = \mu$.

(4) As in (3), if $Z^r_\chi(P,\lambda) \cong Z^r_\chi(\widetilde{P},\mu)$ then $Z_\chi(\lambda) \cong Z_\chi(\mu)$. Hence, by Proposition 10.5 in [Jantzen, 1997], $\lambda \in W \bullet \mu + pX$.

□

Since all irreducible $U^{[r]}(G)$-modules have finite dimension, we can determine $\sup\{\dim(M) \mid M \in \mathrm{Irr}(U^{[r]}(G))\}$, the maximal dimension of an irreducible $U^{[r]}(G)$-module.

Corollary 4.1.4.2. *The maximal dimension of an irreducible $U^{[r]}(G)$-module is $p^{(r+1)\dim(\mathfrak{n}^-)}$, and it is attained.*

Proof. Since every irreducible $U^{[r]}(G)$-module is an irreducible quotient of $Z^r_\chi(P,\lambda)$ for some $\chi \in \mathfrak{g}^*$, $\lambda \in \Lambda_\chi$, and irreducible $\mathrm{Dist}(G_r)$-module P, and since the dimension of $Z^r_\chi(P,\lambda)$ depends only on P, the maximal dimension of an irreducible $U^{[r]}(G)$-module is at most

$$\max_{P \in \mathrm{Irr}(\mathrm{Dist}(G_r))}\{\dim(Z^r_\chi(P,\lambda))\} = \max_{P \in \mathrm{Irr}(\mathrm{Dist}(G_r))}\{(p^{\dim(\mathfrak{n}^-)}\dim(P))\}.$$

The maximal dimension of an irreducible $\mathrm{Dist}(G_r)$-module is $p^{r\dim(\mathfrak{n}^-)}$, coming from the Steinberg weight St.[94] In particular, if we choose $P = L_r(St)$ and χ regular, then $Z^r_\chi(P,\lambda)$ is an irreducible $U^{[r]}(G)$-module of dimension $p^{(r+1)\dim(\mathfrak{n}^-)}$, and the result follows. □

[94]Recall that the Steinberg weight is $(p^r - 1)\rho$, where ρ is the half-sum of all positive roots.

Recall further that, given $x \in \mathfrak{g}$, there exist $x_s, x_n \in \mathfrak{g}$ such that $x = x_s + x_n$, the element x_s is semisimple in $\mathfrak{g}$, the element x_n is nilpotent in $\mathfrak{g}$ and $[x_s, x_n] = 0$. We call $x = x_s + x_n$ a **Jordan decomposition** of x. If, under the G-module isomorphism $\mathfrak{g} \to \mathfrak{g}^*$, we have that x maps to χ, that x_s maps to χ_s and that x_n maps to χ_n, we call $\chi = \chi_s + \chi_n$ a Jordan decomposition of χ.

Given $\chi \in \mathfrak{g}^*$, we define $\mathfrak{c}_{\mathfrak{g}}(\chi) := \{y \in \mathfrak{g} \mid \chi([\mathfrak{g}, y]) = 0\}$. Under our assumptions, $C_G(\chi_s)$ is a Levi subgroup of G with Lie algebra $\mathfrak{c}_{\mathfrak{g}}(\chi_s)$.[95] Hence, there exists a parabolic subgroup[96] P_{χ_s} of G which is a semi-direct product of $C_G(\chi_s)$ with its unipotent radical $U_{P_{\chi_s}}$. Letting $\mathfrak{u} = \mathrm{Lie}(U_{P_{\chi_s}})$ and $\mathfrak{p} = \mathrm{Lie}(P_{\chi_s})$, we get that $\mathfrak{p} = \mathfrak{c}_{\mathfrak{g}}(\chi_s) \oplus \mathfrak{u}$. Work of [Friedlander and Parshall, 1988] shows that there is a equivalence of categories

$$\mathrm{mod}(U_\chi(\mathfrak{g})) \longleftrightarrow \mathrm{mod}(U_\chi(\mathfrak{c}_{\mathfrak{g}}(\chi_s)))$$

which sends $N \in \mathrm{mod}(U_\chi(\mathfrak{g}))$ to the fixed point set $N^{\mathfrak{u}} \in \mathrm{mod}(U_\chi(\mathfrak{c}_{\mathfrak{g}}(\chi_s)))$, and sends $V \in \mathrm{mod}(U_\chi(\mathfrak{c}_{\mathfrak{g}}(\chi_s)))$ to $U_\chi(\mathfrak{g}) \otimes_{U_\chi(\mathfrak{p})} V \in \mathrm{mod}(U_\chi(\mathfrak{g}))$, where $\mathfrak{u}$ acts on V as 0.

Furthermore, letting $\mu = \chi|_{\mathfrak{c}_{\mathfrak{g}}(\chi_s)}$, there is another equivalence of categories

$$\mathrm{mod}(U_\mu(\mathfrak{c}_{\mathfrak{g}}(\chi_s)) \longleftrightarrow \mathrm{mod}(U_{\mu_n}(\mathfrak{c}_{\mathfrak{g}}(\chi_s)))$$

which sends $V \in \mathrm{mod}(U_\mu(\mathfrak{c}_{\mathfrak{g}}(\chi_s)))$ to $V \otimes W \in \mathrm{mod}(U_{\mu_n}(\mathfrak{c}_{\mathfrak{g}}(\chi_s)))$ and then sends $V \in \mathrm{mod}(U_{\mu_n}(\mathfrak{c}_{\mathfrak{g}}(\chi_s)))$ to $V \otimes W^* \in \mathrm{mod}(U_\mu(\mathfrak{c}_{\mathfrak{g}}(\chi_s)))$, where W is a (necessarily 1-dimensional) irreducible $U_{\mu_s}(\mathfrak{c}_{\mathfrak{g}}(\chi_s)/[\mathfrak{c}_{\mathfrak{g}}(\chi_s), \mathfrak{c}_{\mathfrak{g}}(\chi_s)])$-module viewed as a $\mathfrak{g}$-module.

Both of these equivalences of categories send baby Verma modules to baby Verma modules.

Corollary 4.1.4.3. *Keep the notation from the preceding paragraph. There is a bijection*

$$\Psi_\chi : \underline{\mathrm{Irr}}(U_\chi^{[r]}(G)) \xrightarrow{\sim} \underline{\mathrm{Irr}}(\mathrm{Dist}(G_r)) \times \underline{\mathrm{Irr}}(U_{\mu_n}(\mathfrak{c}_{\mathfrak{g}}(\chi_s)))$$

which sends M to $(P, \mathrm{Hom}_{G_r}(P, M)^{\mathfrak{u}} \otimes W^*)$, where P is the unique (up to isomorphism) irreducible $\mathrm{Dist}(G_r)$*-submodule of M. The inverse map sends (P, V) to*

$$(U_\chi^{[r]}(G) \otimes_{\mathrm{Dist}(G_r)} P) \otimes_{U_\chi(\mathfrak{p})} (V \otimes W) \cong P \otimes_{\mathbb{K}} (U_\chi(\mathfrak{g}) \otimes_{U_\chi(\mathfrak{p})} (V \otimes W)).$$

In particular, this result means that to study the irreducible $U_\chi^{[r]}(G)$-modules, one may always assume that $\chi|_{\mathfrak{c}_{\mathfrak{g}}(\chi_s)}$ is nilpotent, and hence that χ vanishes on $\mathfrak{b} \cap \mathfrak{c}_{\mathfrak{g}}(\chi_s)$.

Recall that we say that $\chi \in \mathfrak{g}^*$ has **standard Levi form** if $\chi(\mathfrak{b}) = 0$ and there exists a subset $I \subseteq \Pi$ with $\chi(\mathbf{e}_{-\alpha}) = 0$ if and only if $\alpha \in \Phi^+ - I$.

[95] See [Brown and Gordon, 2001, Lemma 3.2].

[96] Recall that a **parabolic subgroup** of G is a closed subgroup containing a Borel subgroup.

Definition. *We say that* $\chi \in \mathfrak{g}^*$ *has* **almost standard Levi form** *if* $(\chi|_{\mathfrak{c}_{\mathfrak{g}}(\chi_s)})_n$ *has standard Levi form.*

Proposition 4.1.4.4. *Suppose that* $\chi \in \mathfrak{g}^*$ *has almost standard Levi form. Let* $P \in \mathrm{Irr}(\mathrm{Dist}(G_r))$ *and* $\lambda \in \Lambda_\chi$. *Then the* $U_\chi^{[r]}(G)$*-module* $Z_\chi^r(P,\lambda)$ *has a unique irreducible quotient.*

Proof. Since $\mu_n := (\chi|_{\mathfrak{c}_{\mathfrak{g}}(\chi_s)})_n$ has standard Levi form, each $Z_{\mu_n}(\tau)$ for $\tau \in \Lambda_{\mu_n}$ has a unique irreducible quotient. Since there is an equivalence of categories between $\mathrm{mod}(U_{\mu_n}(\mathfrak{c}_{\mathfrak{g}}(\chi_s)))$ and $\mathrm{mod}(U_\chi(\mathfrak{g}))$ which sends baby Verma modules to baby Verma modules, it follows that each $Z_\chi(\lambda)$ has a unique irreducible quotient. The result then follows from Proposition 4.1.3.6. $\square$

If $\chi \in \mathfrak{g}^*$ has almost standard Levi form, we write $L_\chi^r(P,\lambda)$ for the unique irreducible quotient of $Z_\chi^r(P,\lambda)$. Proposition 10.8 in [Jantzen, 1997] gives the following isomorphism condition on these modules, where W_I is the subgroup of the Weyl group generated by simple reflections corresponding to simple roots in I.

Corollary 4.1.4.5. *Suppose that* $\chi \in \mathfrak{g}^*$ *has almost standard Levi form corresponding to the subset* I *of the simple roots of* $\mathfrak{c}_{\mathfrak{g}}(\chi_s)$. *Let* $P, Q \in \mathrm{Irr}(\mathrm{Dist}(G_r))$ *and* $\lambda, \widetilde{\lambda} \in \Lambda_\chi$. *Then* $L_\chi^r(P,\lambda) \cong L_\chi^r(Q,\widetilde{\lambda})$ *if and only if* $P \cong Q$ *and* $\widetilde{\lambda} \in W_I \bullet \lambda$.[97]

4.2 The Azumaya locus of $U^{[r]}(G)$

4.2.1 Azumaya and pseudo-Azumaya loci

Let R be a $\mathbb{K}$-algebra, where $\mathbb{K}$ is an algebraically closed field,[98] which is module-finite over its centre $Z = Z(R)$. Suppose further that Z is an affine $\mathbb{K}$-algebra.[99] One can observe that these conditions guarantee the existence of a bound on the dimensions of irreducible R-modules.[100]

These conditions further imply that R is a PI ring, i.e. that there exists a (multilinear[101]) $\mathbb{Z}$-polynomial f such that $f(r_1,\ldots,r_k) = 0$ for all $r_1,\ldots,r_k \in R$. For $n \in \mathbb{N}$, we define the polynomial g_n as in Chapter 1.4 of [Rowen, 1980].[102] This is an n^2-normal polynomial.[103] We then say that R has **PI-degree** m if R satisfies all multilinear identities of $M_m(\mathbb{Z})$ (that is to say, all multilinear $\mathbb{Z}$-polynomials which vanish on $M_m(\mathbb{Z})$) and

$$g_m(R) := \{g_m(r_1,\ldots,r_k) \,|\, r_1,\ldots,r_k \in R\}$$

[97]Defining $2\rho := \sum_{\alpha\in\Phi^+}\alpha$, we denote $w \bullet \lambda = w(\lambda+\rho) - \rho$, for $w \in W_I$.
[98]In this subsection, we may assume $\mathbb{K}$ to be of arbitrary characteristic.
[99]That is to say, Z is finitely generated as a $\mathbb{K}$-algebra.
[100]See, for example, the proof of Theorem A.4 in [Jantzen, 2004]; although this theorem concerns the universal enveloping algebra of a Lie algebra, the argument works in this greater generality.
[101]Recall that a polynomial in k variables is called multilinear if it is linear in each variable.
[102]See Proposition 1.4.10 in particular.
[103]The polynomial g_n being called n^2**-normal** means g_n is linear and alternating in its first n^2 variables.

is not the zero set. If R has PI-degree m, then $g_m(r_1, \ldots, r_k) \in Z$ for all $r_1, \ldots, r_k \in R$.

We define the following sets:

$$\mathrm{Spec}_m(R) := \{P \in \mathrm{Spec}(R) \mid g_m(R) \nsubseteq P\},$$

$$\mathrm{Spec}_m(Z) := \{Q \in \mathrm{Spec}(Z) \mid g_m(R) \nsubseteq Q\},$$

where $\mathrm{Spec}(R)$ is treated here as just the set of prime ideals[104] in R. One can check that, if R has PI-degree m and P is a prime ideal of R, we have PI-degree$(R) \geqslant$ PI-degree(R/P) and this inequality is an equality precisely when $P \in \mathrm{Spec}_m(R)$.

Given a prime ideal Q in Z, we define R_Q to be the localization of R at the multiplicatively closed central subset $Z - Q$.[105] In other words, $R_Q := \{rs^{-1} \mid r \in R, s \in Z - Q\}$, where $r_1 s_1^{-1} = r_2 s_2^{-1}$ if and only if there exists $s \in Z - Q$ such that $s(r_1 s_2 - r_2 s_1) = 0$. We denote by Z_Q the usual localization of $R - Q$ in Z. By [Rowen, 1980], $Z_Q \subseteq Z(R_Q)$ with equality if $Z - Q$ is regular in R.[106]

Given a central subalgebra C of R, we say[107] that R is **Azumaya** over C if

(i) R is a faithful and finitely generated projective C-module; and

(ii) the canonical map $R \otimes_C R^{op} \to \mathrm{End}_C(R)$, which sends $a \otimes b$ to the map $x \mapsto axb$, is a $\mathbb{K}$-algebra isomorphism.

If $C = Z$, we will simply call R an Azumaya algebra. We furthermore say that R is Azumaya over C **of constant rank** t if R_I is a free module of rank t over C_I for all prime ideals I of C.[108] By Remark 1.8.36 in [Rowen, 1991], we observe that if R is Azumaya over C of constant rank t then, for each prime ideal I of C, we have that R_I is also Azumaya over C_I of constant rank t.

Note that Theorem 5.3.24 in [Rowen, 1991] implies that if R_Q is Azumaya over Z_Q then $Z_Q = Z(R_Q)$. The following lemma follows from Section 5.3 in [Rowen, 1991].

Lemma 4.2.1.1. *The algebra R_Q is Azumaya over Z_Q if and only if $Z_Q = Z(R_Q)$ and R_Q is Azumaya over its centre. Either of these conditions is satisfied if, for example, $Z - Q$ is regular in R and R_Q is Azumaya over its centre.*

The **Azumaya locus** $\mathcal{A}_R$ of R is hence defined to be the set of maximal ideals $\mathfrak{m}$ in Z such that $R_\mathfrak{m}$ is an Azumaya algebra over $Z_\mathfrak{m}$. If R is prime, this is precisely the definition of Azumaya locus given in [Brown and Goodearl, 1997].

---

[104] Recall that a proper ideal P of R is called prime if one of four equivalent conditions holds: (1) if a pair of ideals A, B in R satisfy $AB \subseteq P$ then $A \subseteq P$ or $B \subseteq P$; (2) if a pair of left ideals A, B in R satisfy $AB \subseteq P$ then $A \subseteq P$ or $B \subseteq P$; (3) if a pair of right ideals A, B in R satisfy $AB \subseteq P$ then $A \subseteq P$ or $B \subseteq P$; (4) if a pair of elements $a, b \in R$ satisfy $aRb \subseteq P$ then $a \in P$ or $b \in P$.

[105] If Q is instead an ideal in a subalgebra C of Z, we can of course apply the same construction with C in place of Z.

[106] $Z - Q$ is **regular** in R if for any $s \in Z - Q$, $r \in R$, we have that $sr = 0$ implies $r = 0$.

[107] See, for example, Definition 5.3.23 in [Rowen, 1991].

[108] See Definition 2.12.21 in [Rowen, 1991].

We further define the **pseudo-Azumaya locus** of R, denoted $\mathcal{PA}_R$, as

$$\mathcal{PA}_R := \{\mathrm{ann}_Z(M) \mid M \text{ an irreducible left } R\text{-module of maximal dimension}\}.$$

This is in fact an open subset of $\mathrm{Maxspec}(Z)$. The next theorems show how the Azumaya and pseudo-Azumaya loci are connected.

Theorem 4.2.1.2. *Let R be a $\mathbb{K}$-algebra, where $\mathbb{K}$ is an algebraically closed field, which is module-finite over its centre $Z = Z(R)$, and assume that Z is affine. Let $J(R)$ be the Jacobson radical of R. Then the following results hold.*

(1) *The ring $R/J(R)$ has PI-degree d, where d is the maximal dimension of an irreducible (left) R-module.*

(2) *If R has PI-degree m, then $m = d$ if and only if there exists a primitive ideal A in $\mathrm{Spec}_m(R)$.*

Proof. (1) Observe that for an irreducible R-module M with annihilator $A = \mathrm{ann}_R(M)$, we have that R/A is a finite-dimensional, simple algebra over $Z/\mathfrak{m}$, where $\mathfrak{m} = A \cap Z$. This holds because M is a faithful R/A-module, so R/A embeds in $\mathrm{End}_{\mathbb{K}}(M)$. In particular, $R/A \cong M_{n_A}(\mathbb{K})$ by the algebraically closed nature of the field $\mathbb{K}$, for some $n_A \in \mathbb{N}$. Hence, every irreducible R/A-module has dimension n_A. In particular,

$$d = \max_{A \lhd R \text{ primitive}} \{n_A\}.$$

Furthermore, Kaplansky's Theorem[109] tells us that, for a primitive ideal A of R, the PI-degree of R/A is also n_A. Hence, for any primitive ideal A,

$$\text{PI-degree}(R/A) = n_A \leqslant d.$$

In particular, this says that if f is a multilinear identity of $M_d(\mathbb{Z})$ then $f(R) \subseteq A$ for each primitive ideal A of R. Thus $R/J(R)$ satisfies all the multilinear identities of $M_d(\mathbb{Z})$.

Also, $\text{PI-degree}(R/\mathrm{ann}_R(M)) = d$ if M is an irreducible R-module of maximal dimension. Hence $g_d(R) \subsetneq \mathrm{ann}_R(M)$, and thus $g_d(R) \subsetneq J(R)$. So $g_d(R/J(R)) \neq 0$.

This precisely says that $R/J(R)$ has PI-degree d.

(2) We know that $\text{PI-degree}(R/\mathrm{ann}_R(M)) = d$ when M is an irreducible left R-module of maximal dimension. Thus, $\text{PI-degree}(R) = \text{PI-degree}(R/\mathrm{ann}_R(M))$ when $m = d$, and so $\mathrm{ann}_R(M) \in \mathrm{Spec}_m(R)$.

On the other hand, if there exists a primitive ideal $A \in \mathrm{Spec}_m(R)$ then

$$m = \text{PI-degree}(R) = \text{PI-degree}(R/A) \leqslant \text{PI-degree}(R/J(R)) \leqslant \text{PI-degree}(R)$$

[109]**Kaplansky's Theorem:** If R is a primitive PI ring then R has some PI-degree n and $R \cong M_t(\mathbb{D})$ for a division ring $\mathbb{D}$, uniquely defined up to isomorphism, such that $n^2 = t^2[\mathbb{D} : Z(\mathbb{D})]$. See [Rowen, 1991] for more details.

and the result follows. $\square$

Proposition 4.2.1.3. *Let R be a $\mathbb{K}$-algebra, where $\mathbb{K}$ is an algebraically closed field, which is module-finite over its centre $Z = Z(R)$, and assume that Z is affine. Assume further that R has PI-degree d, where d is the maximal dimension of an irreducible (left) R-module. Then $\mathcal{PA}_R$ is an open subset of* $\mathrm{Maxspec}(Z)$.

Proof. Proposition III.1.1 and Lemma III.1.5 in [Brown and Goodearl, 2002] show that the centre Z is a Noetherian ring and that it is thus enough to show that

$$\widehat{\mathcal{PA}_R} := \{\mathrm{ann}_R(M) \mid M \text{ an irreducible left } R\text{-module of maximal dimension}\}$$

is closed in $\mathrm{Maxspec}(R)$. This is precisely the set of maximal ideals A in R such that $A \in \mathrm{Spec}_d(R)$, using the proof of Theorem 4.2.1.2 and the fact that primitive and maximal ideals are the same in a PI ring. If I is the intersection of all maximal ideals in R which do not lie in $\mathrm{Spec}_d(R)$, then clearly $g_d(R) \subseteq I$. In particular, $I \neq 0$. Furthermore, if A is a maximal ideal of R containing I then $g_d(R) \subseteq A$ and so $A \notin \mathrm{Spec}_d(R)$. Thus

$$\widehat{\mathcal{PA}_R} = \{A \in \mathrm{Maxspec}(R) \mid I \nsubseteq A\},$$

which gives the result. $\square$

Note that the assumptions of Theorem 4.2.1.2 guarantee that R is a Jacobson ring, i.e. that every prime ideal is an intersection of primitive ideals. In particular, $J(R)$ is the intersection of all prime ideals in R. Hence, if R is a prime ring then R has PI degree d and the Azumaya and pseudo-Azumaya loci coincide by the following theorem (noting that, over a prime ring, if $R_{\mathfrak{m}}$ is an Azumaya algebra then it must be of constant rank as $Z(R_{\mathfrak{m}}) = Z_{\mathfrak{m}}$ is local for all maximal ideals $\mathfrak{m}$ of Z – see also Section 13.7 in [McConnell and Robson, 2001]). Note that Brown and Goodearl have already shown the prime case in [Brown and Goodearl, 1997], using similar techniques.

Theorem 4.2.1.4. *Let R be a $\mathbb{K}$-algebra, where $\mathbb{K}$ is an algebraically closed field, which is module-finite over its centre $Z = Z(R)$, and assume that Z is affine. Suppose that R has PI-degree d, where d is the maximum dimension of an irreducible (left) R-module. Furthermore, let M be an irreducible (left) R-module, $A = \mathrm{ann}_R(M)$ and $\mathfrak{m} = \mathrm{ann}_Z(M)$. Then $\dim(M) = d$ if and only if $R_{\mathfrak{m}}$ is an Azumaya algebra of constant rank d^2.*

Note that, since Z is affine, $\mathfrak{m}$ is a maximal ideal of Z.

Proof. ($\Longrightarrow$) Suppose that M is an irreducible (left) R-module of dimension d. Then $R/A \cong M_d(\mathbb{K})$ and so $\text{PI-degree}(R/A) = d = \text{PI-degree}(R)$.

In particular, this means that $A \in \mathrm{Spec}_d(R)$ and so $g_d(R) \nsubseteq A$. Thus, $g_d(R) \cap (Z - \mathfrak{m}) \neq \varnothing$, and hence $g_d(R)$ contains an invertible element of $Z_{\mathfrak{m}}$, so an invertible element of $R_\mathfrak{m}$. Thus $g_d(R_\mathfrak{m}) \neq \{0\}$. Furthermore, any homogeneous multilinear polynomial identity of R is a polynomial identity of $R_\mathfrak{m}$, and so PI-degree$(R_\mathfrak{m})$ = PI-degree(R).

Also, $1 \in g_d(R_\mathfrak{m})R_\mathfrak{m}$ since $g_d(R_\mathfrak{m})$ contains an element of $Z - \mathfrak{m}$. So by a version of the Artin-Procesi theorem (see [Rowen, 1991][110]), $R_\mathfrak{m}$ is Azumaya over its centre of constant rank d^2.

($\Longleftarrow$) Suppose that $R_\mathfrak{m}$ is Azumaya of constant rank d^2 over its centre. In particular, the Artin-Procesi theorem from [Rowen, 1991] tells us that $R_\mathfrak{m}$ has PI-degree d and that $1 \in g_d(R_\mathfrak{m})R_\mathfrak{m}$.

Note that it is always true that $R/\mathfrak{m}R \cong R_\mathfrak{m}/\mathfrak{m}R_\mathfrak{m}$. Furthermore $R_\mathfrak{m}/\mathfrak{m}R_\mathfrak{m}$ satisfies all multilinear identities of $R_\mathfrak{m}$, and if $g_d(R_\mathfrak{m}) \subseteq \mathfrak{m}R_\mathfrak{m}$ then $1 \in g_d(R_\mathfrak{m})R_\mathfrak{m} \subseteq \mathfrak{m}R_\mathfrak{m}$. But then $\mathfrak{m}R_\mathfrak{m} = R_\mathfrak{m}$ which is a contradiction. So $R_\mathfrak{m}/\mathfrak{m}R_\mathfrak{m}$ has PI-degree d, and so $R/\mathfrak{m}R$ has PI-degree d. This precisely says that $\mathfrak{m}R \in \mathrm{Spec}_d(R)$, and so $\mathfrak{m} \in \mathrm{Spec}_d(Z)$.

Since $\mathfrak{m}$ is a maximal ideal of Z, Theorem 1.9.21 of [Rowen, 1980] says that $\mathfrak{m}R$ is a maximal ideal of R, and so $A = \mathfrak{m}R$. In particular, $R/\mathfrak{m}R \cong M_d(\mathbb{K})$ as in the proof of Theorem 4.2.1.2. Since M is an irreducible $R/\mathfrak{m}R$-module, the result follows.

□

Observe that, by Schur's lemma, if M is an irreducible R-module then each $u \in Z$ acts on M by scalar multiplication. In particular, there exists a central character $\zeta_M : Z \to \mathbb{K}$ where $\zeta_M(u)$ is defined by $u \cdot m = \zeta_M(u)m$ for all $m \in M$. Thus,

$$\mathcal{PA}_R = \{\ker(\zeta_M) \mid M \text{ an irreducible } R\text{-module of maximal dimension}\}.$$

4.2.2 Pseudo-Azumaya loci for higher universal enveloping algebras

From now on, we once again suppose $\mathbb{K}$ has characteristic $p > 0$.

We now explore the pseudo-Azumaya locus for the higher universal enveloping algebras. Suppose that G is a connected reductive algebraic group over $\mathbb{K}$. We then take $Z_p^{[r]}$ to be the (central) subalgebra of $U^{[r]}(G)$ generated by the elements $\delta^{\otimes p} - \delta^p$ for $\delta \in \mathrm{Dist}^+_{p^r}(G)$. We know that

$$Z_p^{[r]} = \mathbb{K}\left[(\mathbf{e}_\alpha^{(p^r)})^{\otimes p},\, \binom{\mathbf{h}_t}{p^r}^{\otimes p} - \binom{\mathbf{h}_t}{p^r} \mid \alpha \in \Phi,\, 1 \leqslant t \leqslant d\right].$$

Furthermore, $U^{[r]}(G)$ is an affine $\mathbb{K}$-algebra and a free $Z_p^{[r]}$-module of finite rank $p^{(r+1)\dim(\mathfrak{g})}$. Since $Z_p^{[r]}$ is Noetherian and finitely-generated, the Artin-Tate

[110] In relevant part, this version of the **Artin-Procesi Theorem** says that a ring R is Azumaya of constant rank d^2 if and only if it has PI-degree d and $1 \in g_d(R)R$.

Lemma[111] gives that the centre of $U^{[r]}(G)$, which we denote by $Z^{[r]}(G)$, is an affine $Z_p^{[r]}$-algebra and an affine $\mathbb{K}$-algebra. This implies that $Z_p^{[r]}$, $Z^{[r]}(G)$ and $U^{[r]}(G)$ are Noetherian PI rings and that $U^{[r]}(G)$ is a Jacobson ring.[112]

For the remainder of this chapter we use the convention that for an irreducible $U(\mathfrak{g})$-module N the corresponding central character is $\zeta_N : Z(\mathfrak{g}) \to \mathbb{K}$ while for an irreducible $U^{[r]}(G)$-module M the corresponding central character is $\zeta_M^{[r]} : Z^{[r]}(G) \to \mathbb{K}$. In order to understand how these maps interact, we need to consider some homomorphisms between the centres.

Recall from Subsection 3.2.2 that there exists a surjective algebra homomorphism $\Upsilon := \Upsilon_{r,r} : U^{[r]}(G) \to U(\mathfrak{g})$. This map clearly maps centres to centres, so gives an algebra homomorphism $\Upsilon : Z^{[r]}(G) \to Z(\mathfrak{g})$. In particular, Corollary 3.2.2.3 shows that, $\Upsilon((\mathbf{e}_\alpha^{(p^r)})^{\otimes p}) = \mathbf{e}_\alpha^p$ for $\alpha \in \Phi$ and $\Upsilon(\binom{\mathbf{h}_t}{p^r}^{\otimes p} - \binom{\mathbf{h}_t}{p^r}) = \mathbf{h}_t^p - \mathbf{h}_t$ for $1 \leqslant t \leqslant d$. Hence, Υ further restricts to an algebra homomorphism

$$\Upsilon : Z_p^{[r]} \to Z_p$$

which is now clearly an isomorphism.

There is another map between centres which is worth considering. Let P be an irreducible $\mathrm{Dist}(G_r)$-module, and let us consider the induced module $U^{[r]}(G) \otimes_D P$, where, as always, D denotes $\mathrm{Dist}(G_r)$. The action of $U^{[r]}(G)$ on $U^{[r]}(G) \otimes_D P$ is by left multiplication, so in particular $u \in Z^{[r]}(G)$ acts on $U^{[r]}(G) \otimes_D P$ by the $U^{[r]}(G)$-module endomorphism

$$\rho(u) : U^{[r]}(G) \otimes_D P \to U^{[r]}(G) \otimes_D P,$$

which is left multiplication by u. Clearly $\rho(u)$ is a central element of the algebra $E := \mathrm{End}_{U^{[r]}(G)}(U^{[r]}(G) \otimes_D P)^{op}$. Recall from Lemma 4.1.1.4 that $U(\mathfrak{g})$ is isomorphic to E, and let $\tau : E \to U(\mathfrak{g})$ be the isomorphism. Hence, there is a homomorphism of algebras

$$\Omega_P : Z^{[r]}(G) \to Z(\mathfrak{g})$$

given by composition of τ and ρ.

We can furthermore observe that the proof of Proposition 4.1.2.1 shows that

$$\Omega_P((\mathbf{e}_\alpha^{(p^r)})^{\otimes p}) = \mathbf{e}_\alpha^p$$

for $\alpha \in \Phi$ and

$$\Omega_P\left(\binom{\mathbf{h}_t}{p^r}^{\otimes p} - \binom{\mathbf{h}_t}{p^r}\right) = \mathbf{h}_t^p - \mathbf{h}_t$$

for $1 \leqslant t \leqslant d$. In particular, $\Upsilon|_{Z_p^{[r]}} = \Omega_P|_{Z_p^{[r]}}$, and so Ω_P restricts to an isomorphism

[111] **Artin-Tate Lemma:** Let C be a commutative Noetherian ring and A an affine C-algebra. Let B be a central C-subalgebra of A such that A is a finitely generated B-module. Then B is affine as a C-algebra.

[112] See, for example, Proposition III.1.1 in [Brown and Goodearl, 2002].

$Z_p^{[r]} \to Z_p$.

The following conditions for the map Ω_P to be surjective or injective are easy to prove.

Lemma 4.2.2.1. *The homomorphism Ω_P is surjective if and only if every central element of E is left multiplication by some central element of $U^{[r]}(G)$.*

Lemma 4.2.2.2. *The homomorphism Ω_P is injective if and only if, for $u \in Z^{[r]}(G)$, we have that $u \otimes_D z = 0 \in U^{[r]}(G) \otimes_D P$ for all $z \in P$ implies that $u = 0$. Equivalently, if and only if $U^{[r]}(G) \otimes_D P$ is a faithful $Z^{[r]}(G)$-module.*

Let us see how the homomorphisms Ω_P interact with the central characters of irreducible $U^{[r]}(G)$-modules.

Proposition 4.2.2.3. *Let M be an irreducible $U^{[r]}(G)$-module with $\Psi(M) = (P, N)$ for $P \in \mathrm{Irr}(\mathrm{Dist}(G_r))$ and $N \in \mathrm{Irr}(U(\mathfrak{g}))$. Then the following diagram commutes:*

$$\begin{tikzcd} Z^{[r]}(G) \arrow[r, "\zeta_M^{[r]}"] \arrow[d, "\Omega_P"] & \mathbb{K} \\ Z(\mathfrak{g}) \arrow[ur, "\zeta_N"'] & \end{tikzcd}$$

Proof. Recall here that $M = (U^{[r]}(G) \otimes_D P) \otimes_{U(\mathfrak{g})} N$. Now, let $u \in Z^{[r]}(G)$, $v \in U^{[r]}(G)$, $z \in P$ and $n \in N$. Then

$$\begin{aligned} u \cdot (v \otimes_D z) \otimes_{U(\mathfrak{g})} n = \rho(u)(v \otimes_D z) \otimes_{U(\mathfrak{g})} n &= (v \otimes_D z) \cdot \tau(\rho(u)) \otimes_{U(\mathfrak{g})} n \\ &= (v \otimes_D z) \otimes_{U(\mathfrak{g})} \Omega_P(u) \cdot n = \zeta_N(\Omega_P(u))(v \otimes_D z) \otimes_{U(\mathfrak{g})} n \end{aligned}$$

□

Corollary 4.2.2.4. *Let M be an irreducible $U^{[r]}(G)$-module with $\Psi(M) = (P, N)$ for $P \in \mathrm{Irr}(\mathrm{Dist}(G_r))$ and $N \in \mathrm{Irr}(U(\mathfrak{g}))$. Then*

$$\ker \zeta_M^{[r]} = \Omega_P^{-1}(\ker \zeta_N).$$

Recall from Corollary 4.1.4.2 that if M is an irreducible $U^{[r]}(G)$-module corresponding to the pair $(P, N) \in \mathrm{Irr}(\mathrm{Dist}(G_r)) \times \mathrm{Irr}(U(\mathfrak{g}))$ then we have $\dim(M) = \dim(P)\dim(N)$. Hence, an irreducible $U^{[r]}(G)$-module M is of maximal dimension if and only if the corresponding modules P and N are of maximal dimension.

From now on fix P as the r-th Steinberg module of G, hence an irreducible $\mathrm{Dist}(G_r)$-module of maximal dimension. As in Subsection 4.1.2, let Γ_P be the category of irreducible $U^{[r]}(G)$-modules which contain P as an irreducible $\mathrm{Dist}(G_r)$-submodule. Let $\mathrm{Max}\Gamma_P$ denote the full subcategory of Γ_P whose objects are the irreducible $U^{[r]}(G)$-modules of maximal dimension in Γ_P, and let $\mathrm{MaxIrr}(U(\mathfrak{g}))$

similarly denote the full subcategory of $\mathrm{Irr}(U(\mathfrak{g}))$ consisting of irreducible $U(\mathfrak{g})$-modules of maximal dimension. The inverse equivalences of categories $\Psi_P : \Gamma_P \to \mathrm{Irr}(U(\mathfrak{g}))$ and $\Phi_P : \mathrm{Irr}(U(\mathfrak{g})) \to \Gamma_P$ then restrict to inverse equivalences of categories

$$\Psi_P : \mathrm{Max}\Gamma_P \to \mathrm{MaxIrr}(U(\mathfrak{g})) \qquad \text{and} \qquad \Phi_P : \mathrm{MaxIrr}(U(\mathfrak{g})) \to \mathrm{Max}\Gamma_P.$$

We have already seen that, for $M \in \mathrm{Max}\Gamma_P$, we have $\ker(\zeta_M^{[r]}) = \Omega_P^{-1}(\ker(\zeta_{\Psi_P(M)})$. We hence have that

$$\begin{aligned}\mathcal{PA}_{U^{[r]}(G)} &= \{\ker(\zeta_M^{[r]}) \mid M \in \mathrm{MaxIrr}(U^{[r]}(G))\} = \{\ker(\zeta_M^{[r]}) \mid M \in \mathrm{Max}\Gamma_P\} \\ &= \{\Omega_P^{-1}(\ker(\zeta_{\Psi_P(M)})) \mid M \in \mathrm{Max}\Gamma_P\} = \{\Omega_P^{-1}(\ker(\zeta_N)) \mid N \in \mathrm{MaxIrr}(U(\mathfrak{g}))\}.\end{aligned}$$

Proposition 4.2.2.5. *Let P be the r-th Steinberg module St_r of G. There is a surjective morphism $\Omega_P^* : \mathcal{PA}_{U(\mathfrak{g})} \to \mathcal{PA}_{U^{[r]}(G)}$ which sends $\ker(\zeta_N)$ to $\Omega_P^{-1}(\ker(\zeta_N))$.*

Proof. $\Omega_P : Z^{[r]}(G) \to Z(\mathfrak{g})$ is a homomorphism of commutative algebras, so it induces a morphism

$$\Omega_P^* : \mathrm{Spec}(Z(\mathfrak{g})) \to \mathrm{Spec}(Z^{[r]}(G)).$$

This morphism sends $I \in \mathrm{Spec}(Z(\mathfrak{g}))$ to $\Omega_P^{-1}(I) \in \mathrm{Spec}(Z^{[r]}(G))$, so by above restricts to a map $\Omega_P^* : \mathcal{PA}_{U(\mathfrak{g})} \to \mathcal{PA}_{U^{[r]}(G)}$. It is surjective by the above discussion. ☐

Corollary 4.2.2.6. *Let P be the r-th Steinberg module St_r of G. If Ω_P is surjective, then Ω_P^* is a bijection.*

If we instead take P to be an arbitrary irreducible $\mathrm{Dist}(G_r)$-module then Ψ_P and Φ_P still restrict to inverse equivalences of categories between $\mathrm{Max}\Gamma_P$ and $\mathrm{MaxIrr}(U(\mathfrak{g}))$, and we still get the equality

$$\{\ker(\zeta_M^{[r]}) \mid M \in \mathrm{Max}\Gamma_P\} = \{\Omega_P^{-1}(\ker(\zeta_N)) \mid N \in \mathrm{MaxIrr}(U(\mathfrak{g}))\},$$

but the left hand side may no longer be equal to $\mathcal{PA}_{U^{[r]}(G)}$. For example, if P is the trivial 1-dimensional $\mathrm{Dist}(G_r)$-module then Φ_P simply lifts an irreducible $U(\mathfrak{g})$-module N to the irreducible $U^{[r]}(G)$-module N along the natural quotient $U^{[r]}(G) \mapsto U^{[r]}(G)/U^{[r]}(G)\mathrm{Dist}^+(G_r)$. Hence, if N is an irreducible $U(\mathfrak{g})$-module of maximum dimension, then $\ker(\zeta_N)$ is in the pseudo-Azumaya locus of $U(\mathfrak{g})$ (and hence the Azumaya locus, since $U(\mathfrak{g})$ is prime), but $\Omega_P^*(\ker(\zeta_N)) = \ker(\zeta_N^{[r]})$. In particular, $\Omega_P^*(\ker(\zeta_N))$ will contain $Z \cap U^{[r]}(G)\mathrm{Dist}^+(G_r)$, suggesting that it is not the central annihilator of an irreducible $U^{[r]}(G)$-module of maximum dimension.

Chapter 5

Integration of Modules - Stability

In this chapter and Chapter 6, we turn to a different question than the one we have been considering so far. Specifically, we now wish to consider approaches to the *Humphreys-Verma conjecture.*

Conjecture (Humphreys-Verma conjecture[113]). *Let G be a semisimple, simply-connected algebraic group over an algebraically closed field $\mathbb{K}$ of positive characteristic $p > 0$. Let V be a projective, indecomposable G_1-module. Then there exists a G-module which restricts to V as a G_1-module.*

The significance of this conjecture, of course, is that G_1-modules are precisely restricted $\mathfrak{g}$-modules, so this conjecture is really asking about our ability to integrate modules from Lie algebras to algebraic groups. It is currently proved for $p \geqslant 2h-2$, where h is the Coxeter number of G.[114] Our first approach to this question uses stability.

5.1 G-stable modules for abstract groups

5.1.1 Automorphisms of indecomposable modules

Let $\mathbb{B}$ be a finite-dimensional algebra over a field $\mathbb{K}$ (of any characteristic), V a finite-dimensional $\mathbb{B}$-module, $E = \mathrm{End}(V)$ its endomorphism ring, $J = J(E)$ its Jacobson radical,[115] and $H = \mathrm{Aut}(V)$ its automorphism group. We start with the following useful observation:

[113] See, for example, [Humphreys and Verma, 1973], [Humphreys, 1976], [Ballard, 1978], [Donkin, 1982], and [Sobaje, 2017].

[114] See [Jantzen, 1987, II.11.11]. There are various ways to define the Coxeter number of a root system Φ with set of simple roots Π, but perhaps the easiest is as $|\Phi|/|\Pi|$.

[115] Recall that the Jacobson radical $J(R)$ of a ring R is the intersection of all maximal left ideals of R. Equivalently, it is the intersection of all annihilators of simple left R-modules. This is a two-sided ideal in R, and if we instead consider maximal right ideals and simple right R-modules, we obtain the same ideal.

Proposition 5.1.1.1. (1) *The quotient algebra E/J is a division algebra if and only if V is indecomposable.*

(2) *If V is indecomposable and E/J is separable,*[116] *then $H \cong \mathrm{GL}_1(\mathbb{D}) \ltimes U$ where $\mathbb{D} = E/J$ is a division algebra and $U = 1 + J$ is a connected unipotent group.*

(3) *Under the same assumptions as (2), if $\mathbb{D} = \mathbb{K}$, then $H = \mathrm{GL}_1(\mathbb{K}) \times U$.*

Proof. (1) It is a standard fact that a finite length module is indecomposable if and only if its endomorphism ring is local.[117] Since E is finite-dimensional, this is equivalent to E/J being a division ring.

(2) By (1), $\mathbb{D} = E/J$ is a division algebra. Since $\mathbb{D}$ is separable, we can use the Malcev-Wedderburn Theorem[118] to split off the radical, i.e., to realize $\mathbb{D}$ as a subalgebra of E such that $E = \mathbb{D} \oplus J$.

Clearly, $H = \mathrm{GL}_1(E)$. Consider an element $x = d + j$, where $d \in \mathbb{D}$ and $j \in J$. Since $x^n = d^n + j'$ for some $j' \in J$, the element x is nilpotent if and only if $d = 0$. By the Fitting Lemma,[119] $x \in H$ if and only if $d \neq 0$. The key isomorphism is given by the multiplication map:

$$\mathrm{GL}_1(\mathbb{D}) \ltimes U \xrightarrow{\cong} H = \mathrm{GL}_1(E), \quad (d, 1 + j) \mapsto d + dj \ ,$$

$$H = \mathrm{GL}_1(E) \xrightarrow{\cong} \mathrm{GL}_1(\mathbb{D}) \ltimes U, \quad d + j \mapsto (d, 1 + d^{-1}j) \ .$$

It remains to observe that $U = 1 + J$ is a connected unipotent algebraic group. It is connected because it is isomorphic to J as a variety. It is unipotent because each of its elements is unipotent in $\mathrm{GL}(V)$.

(3) The Malcev-Wedderburn decomposition turns J into a $\mathbb{D}$-$\mathbb{D}$-bimodule.[120] Our condition forces $\mathbb{D} \otimes_{\mathbb{K}} \mathbb{D}^{op} = \mathbb{K} \otimes_{\mathbb{K}} \mathbb{K}^{op} = \mathbb{K}$ so that the bimodule structure is just the $\mathbb{K}$-vector space structure. Hence, $\mathrm{GL}_1(\mathbb{D}) = \mathrm{GL}_1(\mathbb{K})$ and U commute. □

5.1.2 (L, H)-Morphs

Let $G \geqslant L$, $K \geqslant H$ be two group-subgroup pairs. Let $N = N_K(H)$ and $C_K(H)$ be the normaliser[121] and the centraliser[122] of H in K. By **an (L, H)-morph from G to K** we understand a function $f : G \to K$ satisfying the following four conditions:

(M1) $f\,|_L$ is a group homomorphism.

(M2) $f(G) \subseteq N_K(H)$.

[116] Recall that a $\mathbb{K}$-algebra A is **separable** if $A \otimes_{\mathbb{K}} \mathbb{F}$ is semisimple for any field extension $\mathbb{F}$ of $\mathbb{K}$.

[117] See, for example, Proposition 3.1 and Theorem 3.7 in [Jacobson, 1989].

[118] See Theorem 6.2.1 in [Drozd and Kirichenko, 1994].

[119] **Fitting Lemma:** Let R be a ring and V an indecomposable R-module of finite length. Let $f \in \mathrm{End}(V)$. Then either f is bijective or f is nilpotent.

[120] Recall that if R and S are $\mathbb{K}$-algebras, an **$R - S$-bimodule** is an additive group M which is a left R-module, a right S-module, and satisfies $(rm)s = r(ms)$ for all $r \in R$, $s \in S$ and $m \in M$. Equivalently, it is a left $R \otimes_{\mathbb{K}} S^{op}$-module.

[121] Recall that $N_K(H)$ is the set of $k \in K$ such that $kHk^{-1} = H$.

[122] Recall that $C_K(H)$ is the set of $k \in K$ such that $khk^{-1} = h$ for all $h \in H$.

(M3) $f(x)f(y) \in f(xy)H$ for all $x, y \in G$.

(M4) $f(L) \subseteq C_K(H)$.

By a **weak (L,H)-morph from G to K** we understand a function $f : G \to K$ satisfying only the first three conditions.

One can observe that a weak (L,H)-morph is just a homomorphism $G \to N/H$ with a choice of lifting to N satisfying an additional condition.[123] For instance, weak $(G,1)$-morphs are the same as homomorphisms $G \to K$ and weak $(1,K)$-morphs are just functions $G \to K$ which preserves the identity. Furthermore, the same statements also hold if we replace weak morphs with morphs in the previous sentence.

Commonly (L,H)-morphs originate from K-G-sets $X = {}_K X_G$, i.e., G acts on the right, K on the left and the actions commute. Let $\theta \in X$ such that its G-orbit is inside its K-orbit. Let H be the stabiliser of θ in K. Choose a section $K/H \to K$ which sends the coset H to 1_K. The composition of the section with the G-orbit map of θ is a function

$$f : G \to K \quad \text{characterised by} \quad {}^{f(x)}\theta = \theta^x \quad \text{for all } x \in G.$$

Lemma 5.1.2.1. *The map f defined above is a $(1,H)$-morph.*

Proof. By definition, ${}^{f(xy)}\theta = \theta^{xy}$. On the other hand, $\theta^{xy} = (\theta^x)^y = ({}^{f(x)}\theta)^y = {}^{f(x)f(y)}\theta$. Hence, $\theta = {}^{f(xy)^{-1}f(xy)}\theta = {}^{f(xy)^{-1}f(x)f(y)}\theta$ and $f(xy)^{-1}f(x)f(y) \in H$.

Now pick $h \in H$. Then ${}^{f(x)^{-1}hf(x)}\theta = {}^{f(x)^{-1}h}\theta^x = {}^{f(x)^{-1}}\theta^x = {}^{f(x)^{-1}f(x)}\theta = \theta$ so that $f(x)^{-1}hf(x) \in H$. $\square$

We would like to identify weak (L,H)-morphs that define the same homomorphisms $G \to N/H$. More precisely, we say that two weak (L,H)-morphs f and f' are equivalent if $f'(x) \in f(x)H$ for all $x \in G$. We denote the set of equivalence classes of weak (L,H)-morphs by $[LH]\mathrm{mo}(G,K)$. Furthermore, given a fixed homomorphism $\theta : L \to K$ we denote by $[LH]^\theta\mathrm{mo}(G,K)$ the set of equivalence classes of those weak (L,H)-morphs that restrict to θ on L.

Let A be an additive abelian group with a G-action (a $\mathbb{Z}G$-module). We consider a subcomplex $(\widetilde{C}^\bullet(G,L;A), d)$ of the standard complex[124] $(C^\bullet(G;A), d)$ that consists of those cochains μ_n that are trivial on L^n, i.e., $\mu_n \mid_{L\times\cdots\times L} \equiv 0_A$.

We observe that this cochain complex fits into an exact sequence of cochain complexes

$$0 \to \widetilde{C}^\bullet(G,L;A) \to C^\bullet(G;A) \to C^\bullet(L;A) \to 0 .$$

[123] Namely that the lifting must remain a homomorphism on L.

[124] The reader should recall that the complex $(C^\bullet(G;A), d)$ consists of abelian groups $C^n(G;A) := \{\mu : G^n \to A\}$, for $n \in \mathbb{N}$, with differentials $d_n : C^n(G;A) \to C^{n+1}(G;A)$ defined by $d_n\mu(g_1,\ldots,g_{n+1}) = g_1\mu(g_2,\ldots,g_{n+1}) + \sum_{i=1}^n \mu(g_1,\ldots,g_{i-1},g_ig_{i+1},g_{i+2},\ldots,g_{n+1}) + \mu(g_1,\ldots,g_n)$ for $\mu \in C^n(G;A)$ and $g_1,\ldots,g_{n+1} \in G$.

This then allows us to form a long exact sequence of cohomology

$$\cdots \to H^{n-1}(L;A) \to \widetilde{H}^n(G,L;A) \to H^n(G;A) \to H^n(L;A) \to \cdots$$

For our purposes, we have to modify this subcomplex slightly. We consider a subcomplex $(C^\bullet(G,L;A),d)$ of the standard complex $(C^\bullet(G;A),d)$ which is obtained from $(\widetilde{C}^\bullet(G,L;A),d)$ in the following way: for $n > 0$, we have $C^n(G,L;A) = \widetilde{C}^n(G,L;A)$, whilst $C^0(G,L;A) = A^L$. We can furthermore replace the complex $C^\bullet(L;A)$ with the complex $\widetilde{C}^\bullet(L;A)$, defined by $\widetilde{C}^n(L;A) = \mathrm{Coker}(C^n(G,L;A) \to C^n(G;A))$ for all $n \geqslant 0$. In particular, we observe that $\widetilde{C}^n(L;A) = C^n(L;A)$ for all $n \geqslant 1$. This then recovers an exact sequence of cochain complexes:

$$0 \to C^\bullet(G,L;A) \to C^\bullet(G;A) \to \widetilde{C}^\bullet(L;A) \to 0 .$$

In particular, noting that for the cochain complex $\widetilde{C}^\bullet(L;A)$ we have $\widetilde{H}^0(L;A) = 0$ and $\widetilde{H}^n(L;A) = H^n(L;A)$ for $n \geqslant 1$, we can form the long exact sequence of cohomology

$$\begin{aligned}0 \to H^1(G,L;A) \to H^1(G;A) \to H^1(L;A) \to \cdots\\ \ldots \to H^{n-1}(L;A) \to H^n(G,L;A) \to H^n(G;A) \to H^n(L;A) \to \cdots\end{aligned}$$

What can we say about the natural map $f_n : H^n(G,L;A) \to H^n(G;A)$? From this long exact sequence, the following proposition is clear.

Proposition 5.1.2.2. (1) *For $n > 0$, $H^n(L;A) = 0$ if and only if f_n is surjective and f_{n+1} is injective.*

(2) *For $n > 1$, the map f_n is injective if and only if the restriction map $Z^{n-1}(G;A) \to Z^{n-1}(L;A)$ is surjective.*

Proof. (1) This follows from the exact sequence.

(2) Suppose $Z^{n-1}(G;A) \to Z^{n-1}(L;A)$ is surjective. Pick $\mu \in Z^n(G,L;A)$ such that $[\mu] \in \ker(f_n)$. Then $\mu \in B^n(G;A)$ and $\mu = d\eta$ for some $\eta \in C^{n-1}(G;A)$. Moreover, $d(\eta|_L) = \mu|_L \equiv 0$ so that $\eta|_L \in Z^{n-1}(L;A)$. Our assumption gives $\zeta \in Z^{n-1}(G;A)$ such that $\zeta|_L = \eta|_L$. Hence, $\eta - \zeta \in C^{n-1}(G,L;A)$ and $\mu = d(\eta - \zeta) \in B^n(G,L;A)$.

Now suppose f_n is injective. Pick $\mu \in Z^{n-1}(L;A)$, and extend it to $\chi \in C^{n-1}(G;A)$. Hence $d\chi \in Z^n(G,L;A)$ and $[d\chi] \in \ker(f_n)$. So $d\chi = d\zeta$ for some $\zeta \in C^{n-1}(G,L;A)$. Now $\chi - \zeta \in Z^{n-1}(G;A)$ and $(\chi - \zeta)|_L = \mu$. □

Corollary 5.1.2.3. *For $n > 1$, $H^n(G,L;A) = 0$ if and only if $H^{n-1}(G;A) \to H^{n-1}(L;A)$ is surjective and $H^n(G;A) \to H^n(L;A)$ is injective. Furthermore, $H^1(G,L;A) = 0$ if and only if $H^1(G;A) \to H^1(L;A)$ is injective.*

The next theorem clarifies the origin of this new complex. Let us fix a homomorphism $\theta = f|_L : L \to N$ and choose a subgroup $\widetilde{H} \leqslant H$, normal in $N = N_K(H)$ such that $A := H/\widetilde{H}$ is abelian. Notice that the conjugation ${}^{gH}h\widetilde{H} := ghg^{-1}\widetilde{H}$ defines a structure of an N/H-module (and a G-module via any weak (L,H)-morph) on A. Informally, we should think of the next theorem as "an exact sequence"

$$H^1(G,L;A) \dashrightarrow [L\widetilde{H}]^\theta\mathrm{mo}(G,N) \longrightarrow [LH]^\theta\mathrm{mo}(G,N) \longrightarrow H^2(G,L;A) \qquad (5.1)$$

keeping in mind that the second and the third terms are sets (not even pointed sets) and the first arrow is an "action" rather than a map. Let us make it more precise: a weak (L,H)-morph defines a G-module structure ρ on A. For each particular ρ (not just its isomorphism class) we define

$$[L\widetilde{H}]^\theta\mathrm{mo}(G,N)_\rho \subseteq [L\widetilde{H}]^\theta\mathrm{mo}(G,N), \quad [LH]^\theta\mathrm{mo}(G,N)_\rho \subseteq [LH]^\theta\mathrm{mo}(G,N)$$

as subsets of those weak (L,H)-morphs that define this particular G-action ρ. These subsets could be empty, in which case we consider the following theorem true for trivial reasons. The reader should consider this theorem and its proof as a generalisation of the results in Sections 1 and 2 in [Thévenaz, 1983] to the situation of weak (L,H)-morphs.

Theorem 5.1.2.4. *We are in the notations preceding this theorem. For each G-action ρ on A the following statements hold:*

(1) *There is a restriction map*

$$\mathrm{Res} : [L\widetilde{H}]^\theta\mathrm{mo}(G,N)_\rho \longrightarrow [LH]^\theta\mathrm{mo}(G,N)_\rho, \quad \mathrm{Res}(\langle f\rangle) = [f]$$

where $\langle f\rangle$ and $[f]$ denote the equivalence classes in $[L\widetilde{H}]^\theta\mathrm{mo}(G,N)_\rho$ and $[LH]^\theta\mathrm{mo}(G,N)_\rho$.

(2) *The abelian group $Z^1(G,L;(A,\rho))$ acts freely on the set $[L\widetilde{H}]^\theta\mathrm{mo}(G,N)_\rho$ by*

$$\gamma\cdot\langle f\rangle := \langle\dot{\gamma}f\rangle \ \text{ where } \ \dot{\gamma}f(x) = \dot{\gamma}(x)f(x) \ \text{ for all } \ x\in G$$

and $\dot{\gamma} : G \xrightarrow{\gamma} A \to H$ is a lift of γ to a map $G\to H$ with $\dot{\gamma}(1) = 1$.

(3) *The corestricted restriction map* $\mathrm{Res} : [L\widetilde{H}]^\theta\mathrm{mo}(G,N)_\rho \longrightarrow \mathrm{Im}(\mathrm{Res})$ *is a quotient map by the $Z^1(G,L;(A,\rho))$-action.*

(4) *Two classes $\langle f\rangle, \langle g\rangle \in [L\widetilde{H}]^\theta\mathrm{mo}(G,N)_\rho$ lie in the same $B^1(G,L;(A,\rho))$-orbit if and only if there exist $h\in H$, $f'\in\langle f\rangle$, $g'\in\langle g\rangle$ such that $[f(L),h]\subseteq\widetilde{H}$ and $f'(x) = hg'(x)h^{-1}$ for all $x\in G$.*

(5) *There is an obstruction map*

$$\mathrm{Obs} : [LH]^\theta\mathrm{mo}(G,N)_\rho \longrightarrow H^2(G,L;(A,\rho)), \quad \mathrm{Obs}([f]) = [f^\sharp]$$

where the cocycle $f^\sharp$ is defined by $f^\sharp(x,y) = f(x)f(y)f(xy)^{-1}\widetilde{H}$.

(6) *The sequence (5.1) is exact, i.e., the image of* Res *is equal to* $\mathrm{Obs}^{-1}([0])$.

Proof. Suppose $\langle f\rangle = \langle g\rangle$. This gives a function $\alpha : G \to \widetilde{H}$ such that $\alpha|_L \equiv 1$ and $f(x) = \alpha(x)g(x)$ for all $x \in G$. Since $H \supseteq \widetilde{H}$, we conclude that $[f] = [g]$ and the map Res is well-defined. This proves (1).

Suppose $\mathrm{Res}(\langle f\rangle) = \mathrm{Res}(\langle g\rangle)$. Then $[f] = [g]$ gives a function $\alpha : G \to H$ such that $\alpha|_L \equiv 1$ and $f(x) = \alpha(x)g(x)$ for all $x \in G$. We can also obtain such a function from a cochain $\gamma \in C^1(G, L; (A, \rho))$ by lifting $\alpha = \dot{\gamma}$. Let us compute in the group $N/\widetilde{H}$ denoting $a\widetilde{H}$ by $\overline{a}$. The weak (L, H)-morph condition for f is equivalent to the following equality:

$$\overline{\alpha(xy)}\;\overline{g(xy)} = \overline{f(xy)} = \overline{f(x)}\;\overline{f(y)} = \overline{\alpha(x)g(x)}\;\overline{\alpha(y)g(y)}$$
$$= \overline{\alpha(x)g(x)\alpha(y)g(x)^{-1}}\;\overline{g(x)g(y)}.$$

Now notice that

$$\overline{g(xy)} = \overline{g(x)g(y)} = \overline{g(x)}\;\overline{g(y)}$$

is the weak (L, H)-morph condition for g, while

$$\overline{\alpha(xy)} = \overline{\alpha(x)g(x)\alpha(y)g(x)^{-1}} = \overline{\alpha(x)}\;\overline{g(x)\alpha(y)g(x)^{-1}} = \overline{\alpha(x)}\;[\rho(x)(\overline{\alpha})](y)$$

is the cocycle condition for $\overline{\alpha} = \alpha\widetilde{H}$. Any two of these three conditions imply the third one, which proves both (2) and (3), except the action freeness.

Suppose $\langle f\rangle = \gamma \cdot \langle f\rangle = \langle \dot{\gamma} f\rangle$. This gives a function $\alpha : G \to \widetilde{H}$ such that $\alpha|_L \equiv 1$ and $\dot{\gamma}(x)f(x) = \alpha(x)f(x)$ for all $x \in G$. Hence, $\dot{\gamma} = \alpha$ and $\gamma = \overline{\alpha} \equiv 1$. Thus, the action is free.

Let us examine $da \cdot \langle f\rangle = \langle \dot{da} f\rangle$ for some $a \in A^L$. Since $da(x) = -a + \rho(x)(a)$ and $\rho(x)$ can be computed by conjugating with $f(x)$, we immediately conclude that

$$[\dot{da} f](x) = \dot{a}^{-1} f(x)\dot{a} f(x)^{-1} f(x) = \dot{a}^{-1} f(x)\dot{a}.$$

It is easy to see that $[f(L), \dot{a}] \subseteq \widetilde{H}$. The argument we have just given is reversible, i.e., if $f(x) = hg(x)h^{-1}$ then $\langle g\rangle = d\overline{h} \cdot \langle f\rangle$ and $\overline{h} \in A^L$. This proves (4).

Suppose $[f] = [g]$. This gives a function $\alpha : G \to H$ such that $\alpha|_L \equiv 1$ and $f(x) = \alpha(x)g(x)$ for all $x \in G$. Let us compute the cocycles in $N/\widetilde{H}$, keeping in mind that $H/\widetilde{H}$ is abelian:

$$f^\sharp(x,y) = \overline{f(x)f(y)f(xy)^{-1}} = \overline{\alpha(x)}\;\overline{g(x)}\;\overline{\alpha(y)}\;\overline{g(y)}\;\overline{g(xy)}^{-1}\overline{\alpha(xy)}^{-1} =$$
$$(\overline{\alpha(xy)}^{-1}\overline{\alpha(x)}\;\overline{g(x)\alpha(y)g(x)^{-1}})\overline{g(x)g(y)g(xy)^{-1}} = d\,\overline{\alpha}(x,y) + g^\sharp(x,y).$$

Thus $[f^\sharp] = [g^\sharp]$, proving (5).

It is clear that $f^\sharp \equiv 1$ for $f \in [L\widetilde{H}]^\theta\mathrm{mo}(G, N)_\rho$. Hence, $\mathrm{Obs}(\mathrm{Res}(\langle f\rangle)) = [0]$.

Suppose now that $\mathrm{Obs}([f]) = [0]$. This gives a function $\alpha : G \to H$ such that $\alpha|_L \equiv 1$ and $d\overline{\alpha} = f^\sharp$ Consider $g : G \to N$ defined by $g(x) = \alpha(x)^{-1}f(x)$ for all $x \in G$. Then $[g] = [f]$ and we can verify that $g \in [L\widetilde{H}]^\theta\mathrm{mo}(G,N)_\rho$ by checking $g^\sharp \equiv 1$ in $N/\widetilde{H}$:

$$g^\sharp(x,y) = \overline{\alpha(x)}^{-1}\overline{f(x)}\,\overline{\alpha(y)}^{-1}\overline{f(y)}\,\overline{f(xy)}^{-1}\overline{\alpha(xy)}$$
$$\sim \overline{\alpha(xy)}\,\overline{\alpha(x)}^{-1}(\overline{f(x)}\,\overline{\alpha(y)}\,\overline{f(x)}^{-1})^{-1}f^\sharp(x,y)$$
$$= (d\,\overline{\alpha}(x,y))^{-1}f^\sharp(x,y) \equiv 1.$$

This proves (6). □

Let us quickly re-examine how the last section works for (L,H)-morphs. All of its results including Theorem 5.1.2.4 clearly work, although the objects that appear have additional properties. Most crucially, since $f(L) \subseteq C_K(H)$, the L-action on the abelian group A is trivial. If L is normal in G, this just means that A is a $\mathbb{Z}G/L$-module.

An important feature is that $Z^1(L;A)$ consists of homomorphisms $L \to A$ in this case. This means that Proposition 5.1.2.2 yields the following corollary:

Corollary 5.1.2.5. *If the group L is perfect, then $f_1 : H^1(G,L;A) \to H^1(G;A)$ is surjective and $f_2 : H^2(G,L;A) \to H^2(G;A)$ is injective.*

5.1.3 Module extensions

We now assume that L is a normal subgroup of G. Let $\mathbb{A}$ be a ring, (V,θ) an $\mathbb{A}L$-module, $K = \mathrm{Aut}_{\mathbb{A}}V$ and $H = \mathrm{Aut}_{\mathbb{A}L}V$ its automorphism groups. We can think of θ as an element of the set of $\mathbb{A}L$-structures $X = \mathrm{Hom}(L,K)$. Then H is the centraliser in K of $\theta(L)$. By N, as before, we denote the normaliser of H in K.

Naturally, X is a K-G-set: G acts by conjugation on L twisting the $\mathbb{A}L$-module structure. K acts by conjugations on the target, while $H = \mathrm{Stab}_K(\theta)$. The module V is called **G-stable** if $(V,\theta) \cong (V,\theta^g)$ for all $g \in G$. This is equivalent to the orbit inclusion $\theta^G \subseteq {}^K\theta$. By Lemma 5.1.2.1 this gives a $(1,H)$-morph $f : G \to K$.

If $g \in L$, the isomorphism $f(g) : (V,\theta) \to (V,\theta^g)$ can be chosen to be $\theta(g)$. Indeed,

$$\theta(g)(\theta(h)v) = \theta(gh)(v) = \theta(ghg^{-1})(\theta(g)(v)) = \theta^g(h)(\theta(g)(v))$$

for all $g,h \in L$. Then, without loss of generality $f|_L = \theta$, and f is an (L,H)-morph in $[LH]^\theta\mathrm{mo}(G,N)$.

Suppose that the group $H = \mathrm{Aut}_{\mathbb{A}L}V$ is soluble. We can always find a subnormal series $H = H_0 \rhd H_1 \rhd \ldots \rhd H_k = \{1\}$ with abelian quotients $A_j = H_{j-1}/H_j$ such that each H_j is normal in N. For instance, we can use the commutator series $H_j = H^{(j)}$. In this case, every abelian group A_j becomes an N-module.

If $\mathbb{A}$ is finite-dimensional over the field $\mathbb{K}$ and V is a finite-dimensional indecomposable $\mathbb{A}L$-module, we can use Proposition 5.1.1.1 to derive useful information about its automorphisms. In particular, if $\mathbb{D} = \mathrm{End}_{\mathbb{A}L}(V)/J$ is a separable field extension of $\mathbb{K}$, then $H = \mathrm{GL}_1(\mathbb{D}) \ltimes (1 + J)$ is soluble. It admits another standard N-stable subnormal series:

$$H_m = 1 + J^m, \ m \geqslant 1, \quad A_m = (1 + J^m)/(1 + J^{m+1}).$$

As groups, we have $A_m = ((1 + J^m)/(1 + J^{m+1}), \cdot) \cong (J^m/J^{m+1}, +)$. The following theorem is the direct application of Theorem 5.1.2.4. It determines the uniqueness and existence of a G-module structure on a G-stable L-module. The proof is obvious.

Theorem 5.1.3.1. *Let $V = (V, \theta)$ be a G-stable $\mathbb{A}L$-module with a soluble automorphism group H, where $\mathbb{A}$ is an associative ring. Let $H = H_0 \rhd H_1 \rhd \ldots \rhd H_k = \{1\}$ be a subnormal N-stable series with abelian factors $A_j = H_{j-1}/H_j$.*

Any $\mathbb{A}G$-module structure Θ on (V, θ) compatible with its $\mathbb{A}L$-structure (i.e., $\Theta|_{\mathbb{A}L} = \theta$) can be discovered by the following recursive process in k steps. One initialises the process with an (L, H_0)-morph $f_0 = f$ coming from the G-stability. The step m is the following.

(1) *The (L, H_{m-1})-morph $f_{m-1} : G \to N$ such that $f_{m-1}|_L = \theta$ determines a G-module structure ρ_m on A_m.*

(2) *If $\mathrm{Obs}([f_{m-1}]) \neq 0 \in H^2(G, L; (A_m, \rho_m))$, then this branch of the process terminates.*

(3) *If $\mathrm{Obs}([f_{m-1}]) = 0 \in H^2(G, L; (A_m, \rho_m))$, then we choose an (L, H_m)-morph $f_m : G \to N$ such that $\mathrm{Res}([f_m]) = [f_{m-1}]$.*

(4) *For each element of $H^1(G, L; (A_m, \rho_m))$ we choose a different f_m branching the process. (The choices different by an element of $B^1(G, L; (A_m, \rho_m))$ are equivalent, not requiring the branching.)*

(5) *We change m to $m + 1$ and go to step (1).*

An $\mathbb{A}G$-module structure Θ on (V, θ) compatible with its $\mathbb{A}L$-structure is equivalent to f_k for one of the non-terminated branches. Distinct non-terminated branches produce (as f_k) non-equivalent compatible $\mathbb{A}G$-module structures.

This process is subtle as ρ_m is revealed only when f_{m-1} is computed. It would be useful to have stability, i.e., the fact the G-modules (A_m, ρ_m) are the same (isomorphic) for different branches. The actions ρ_m on $A_m = H_{m-1}/H_m$ on different branches differ by conjugation via a function $G \to H_{m-2}$. Thus, one needs all two-step quotients H_{m-1}/H_{m+1} to be abelian to ensure stability. Having said that, we can still have some easy criteria for existence, uniqueness and non-uniqueness.

Corollary 5.1.3.2. (Existence Test) *Suppose* $H^2(G, L; (A_m, \rho_m)) = 0$ *for all* m *for one of the branches. Then this branch does not terminate and an* $\mathbb{A}G$*-module structure exists.*

Corollary 5.1.3.3. (Uniqueness Test) *Suppose* $H^1(G, L; (A_m, \rho_m)) = 0$ *for all* m *for one of the non-terminating branches. Then this branch is the only branch. Moreover, if an* $\mathbb{A}G$*-module structure exists, it is unique up to an isomorphism.*

Corollary 5.1.3.4. (Non-Uniqueness Test) *Suppose* $H^1(G, L; (A_k, \rho_k)) \neq 0$ *for one of the non-terminating branches. Then there exist non-equivalent* $\mathbb{A}G$*-module structures.*

5.1.4 Extension from not necessarily normal subgroups

In Subsection 5.1.3 we restrict our attention to the case of L being a normal subgroup of G. Let us take a moment to examine how Subsection 5.1.3 works if L is not normal.

Set $P := \bigcap_{g \in G} L^g$, where $L^g := g^{-1}Lg$. Let $\mathbb{A}$ be a ring, (V, θ) an $\mathbb{A}L$-module. Note that (V, θ) is also an $\mathbb{A}P$-module under restriction, so we can view θ as an element of the set $X = \mathrm{Hom}(P, K)$, where $K = \mathrm{Aut}_{\mathbb{A}}V$. Let $H = \mathrm{Aut}_{\mathbb{A}P}V$, so H is the centraliser in K of $\theta(P)$. By N, as before, we denote the normaliser of H in K.

As in Subsection 5.1.3, X is a K-G-set. The $\mathbb{A}L$-module V is called **G-stable-by-conjugation** if $(V, \theta) \cong (V, \theta^g)$ as $\mathbb{A}[L \cap L^g]$-modules for all $g \in G$. Note that this condition guarantees that V is G-stable as an $\mathbb{A}P$-module. This is equivalent to the orbit inclusion $\theta^G \subseteq {}^K\theta$. By Lemma 5.1.2.1 this gives a $(1, H)$-morph $f : G \to K$.

If $g \in L$, the $\mathbb{A}[L \cap L^g]$-isomorphism $f(g) : (V, \theta) \to (V, \theta^g)$ can be chosen to be $\theta(g)$. Indeed, $\theta(g)(\theta(h)v) = \theta(gh)(v) = \theta(ghg^{-1})(\theta(g)(v)) = \theta^g(h)(\theta(g)(v))$ for $g \in L$, $h \in L \cap L^g$. Then, without loss of generality $f|_L = \theta$, and f is an (L, H)-morph in $[LH]^\theta\mathrm{mo}(G, N)$.

This then allows us to proceed with the inductive process of Theorem 5.1.3.1 as before, when $H = \mathrm{Aut}_{\mathbb{A}P}V$ is soluble.

5.1.5 Comparison with $C^\bullet(G/L; A)$

When studying the question of extending representations from a normal subgroup, [Dade, 1981] and [Thévenaz, 1983] use the cohomology of the familiar cochain complex $(C^\bullet(G/L; A), d)$ to control existence and uniqueness of such extensions. In this subsection, however, we use the cohomology complex $(C^\bullet(G, L; A), d)$ instead. It is worth taking a moment to compare the cohomology of these two complexes, and see where the difference in approaches arises. We use the notation of Subsection 5.1.2, assuming that cochains are normalised since this does not affect the cohomology groups.[125]

[125] A 1-cochain $\mu : G \to A$ is called **normalised** if $\mu(1) = 0$. A 2-cochain $\eta : G \times G \to A$ is called **normalised** if $\eta(1, g) = \eta(g, 1) = 0$ for all $g \in G$.

In order for the action of G/L on A to make sense, we need to make the assumption that L acts on A trivially. The reader can observe that this assumption holds in the case considered in Subsection 5.1.3, and, in fact, holds whenever one obtains the G-action on A from an (L, H)-morph as opposed to a weak (L, H)-morph. With this assumption, we have the following proposition.

Proposition 5.1.5.1. *Under the aforementioned conditions we have isomorphisms of groups* $H^0(G, L; A) \cong H^0(G/L; A)$ *and* $H^1(G, L; A) \cong H^1(G/L; A)$.

Proof. It is easy to see that $H^0(G, L; A) = A^G = H^0(G/L; A)$. The natural map from the group of normalised cochains

$$\mathrm{inf} : \widehat{C}^1(G/L; A) \to C^1(G, L; A), \quad \mathrm{inf}(\mu)(g) = \mu(gL).$$

defines a map $\mathrm{Inf} := [\mathrm{inf}] : H^1(G/L; A) \to H^1(G, L; A)$ of cohomology groups. It is injective because $\mathrm{Inf}([\mu]) = 0$ means that $\mathrm{inf}(\mu) = da$ for some $a \in A$. Then $\mu = da$ and $[\mu] = 0$.

It is surjective because for $\eta \in Z^1(G, L; A)$ we have $d\eta = 0$ that translates as

$$\eta(gh) = {}^g(\eta(h)) + \eta(g) \quad \text{for all} \quad g, h \in G.$$

If one chooses $h \in L$, then it tells us that $\eta(gh) = \eta(g)$, i.e., that η is constant on L-cosets. Thus, the cocycle

$$\mu \in \widehat{Z}^1(G/L; A), \quad \mu(gL) := \eta(g)$$

is well-defined. By definition $\mathrm{inf}(\mu) = \eta$. ☐

Considering the second cohomology of these complexes, it is still possible to construct the inflation map $\mathrm{Inf} : H^2(G/L; A) \to H^2(G, L; A)$ in the natural way, but this map is no longer an isomorphism in general. We can still view $H^2(G/L; A)$ as a subgroup of $H^2(G, L; A)$:

Proposition 5.1.5.2. *The map* $\mathrm{Inf} : H^2(G/L; A) \to H^2(G, L; A)$ *is injective.*

Proof. If $\mathrm{Inf}([\eta]) = 0 \in H^2(G, L; A)$ then there exists $\mu \in C^1(G, L; A)$ such that $d\mu = \mathrm{inf}(\eta)$. Note that $\mathrm{inf}(\eta)$ is constant on $L \times L$-cosets by construction. In particular, for $g \in G$ and $h \in L$, we have

$$\mu(g) - \mu(gh) = {}^g(\mu(h)) + \mu(g) - \mu(gh) = \mathrm{inf}(\eta)(g, h) = \mathrm{inf}(\eta)(g, 1) = 0,$$

using fact that η is normalised for the last equality. Hence, μ is constant on cosets of L in G. In particular, if we define $\widetilde{\mu} \in \widehat{C}^1(G/L; A)$ by $\widetilde{\mu}(gL) = \mu(g)$ then we obtain that $\eta = d\widetilde{\mu}$ and so $[\eta] = 0 \in H^2(G/L; A)$. ☐

In the context of Theorem 5.1.2.4, we can see that $H^2(G/L; A)$ and $H^2(G, L; A)$ can be made to play the same role in certain key cases. To that end, we say that an (L, H)-morph f is **normalised** if $f(gh) = f(g)f(h)$ whenever $g \in G$ and $h \in L$. Note that this definition is independent of the subgroup H.

Lemma 5.1.5.3. *In the context of Theorem 5.1.3.1, the (L, H_i)-morphs f_i can be assumed to be normalised for each i. Furthermore, with this assumption, the cocycles $f_i^\sharp \in Z^2(G, L; A_{i+1})$ are constant on cosets of $L \times L$ in $G \times G$.*

Proof. These results follow easily from Lemmas 9.2 and 9.4(i) in [Karpilovsky, 1989]. □

For the remainder of this subsection we assume that all morphs are normalised. The second statement of Lemma 5.1.5.3 immediately yields that, given an (L, H)-morph f, the element $\mathrm{Obs}([f])$ lies in the image of the natural homomorphism $\mathrm{Inf} : H^2(G/L; A) \to H^2(G, L; A)$. The discussion in this subsection yields the following result.

Corollary 5.1.5.4. *Let f be a normalised (L, H)-morph. Then there exists $\eta \in Z^2(G/L; A)$ with $\mathrm{Inf}([\eta]) = \mathrm{Obs}([f])$. Furthermore, $\mathrm{Obs}([f]) = 0 \in H^2(G, L; A)$ if and only if $[\eta] = 0 \in H^2(G/L; A)$.*

Combining Proposition 5.1.5.1 and Corollary 5.1.5.4, we observe that Chapters 5.1.2 and 5.1.3 could be interpreted using the cochain complex $C^\bullet(G/L; A)$ at all points instead of the complex $C^\bullet(G, L; A)$ (although doing so would force us to work exclusively with normalised morphs instead of not-necessarily-normalised weak morphs). Indeed, this is the approach taken by Dade and Thévenaz in the contexts they consider. Our reasons for not taking this approach are threefold. Firstly, our new complex fits nicely into an exact sequence as described in Subsection 5.1.2. Secondly, this complex is more natural to work with – Dade and Thévenaz essentially move from the complex $C^\bullet(G/L; A)$ to the complex $C^\bullet(G, L; A)$ as described in this subsection, and then proceed as we do. Finally, our main motivation in studying the case for abstract groups is to gain insight into the question for algebraic groups, where the procedures described in this subsection do not work smoothly (cf. Subsection 5.2.5).

In particular, the reader should note that if H is abelian then the corollaries at the end of Subsection 5.1.3 give precisely Corollary 1.8 and Proposition 2.1 in [Thévenaz, 1983].

5.2 G-stable modules for algebraic groups

We return to considering algebraic groups over an algebraically closed field $\mathbb{K}$ of positive characteristic p. In this section, all group schemes will be assumed to be affine, but not necessarily reduced. Furthermore, recall that algebraic groups are affine and reduced by definition, and we shall therefore frequently identify an algebraic group with its $\mathbb{K}$-points, equipped with the Zariski topology.

Similar to the definition for abstract groups, a restricted $\mathfrak{g}$-module if called a **G-stable $\mathfrak{g}$-module** is (V, θ) is isomorphic to $(V, \theta)^x := (V, \theta \circ \mathrm{Ad}(x))$ for all $x \in G$. Here, as always, Ad represents the adjoint action of G on $\mathfrak{g}$ and on the restricted enveloping algebra $U_0(\mathfrak{g})$.

5.2.1 Rational and algebraic G-modules

We distinguish algebraic and rational maps of algebraic varieties.[126] In particular, we talk about algebraic and rational homomorphisms of algebraic groups $f : G \to H$. The latter are defined on an open dense[127] subset $U = \mathrm{dom}(f)$ of G containing 1 and satisfy $f(x)f(y) = f(xy)$ whenever $x, y, xy \in U$.

A **rational automorphic G-action** on a commutative algebraic group H is a rational map $G \times H \to H$, defined on an open set $U \times H$ containing $1 \times H$, with the usual action conditions and also such that for each $g \in U$ the map $x \mapsto {}^g x$ is a group automorphism of H. An **algebraic G-action** on H is the same, but where the map $G \times H \to H$ is algebraic.

In an important case, the distinction between rational and algebraic maps can be essentially forgotten, as observed in [Rosenlicht, 1956].

Lemma 5.2.1.1. *[Rosenlicht, 1956, Theorem 3] Let G and H be algebraic groups with G connected. Suppose $f : G \to H$ is a rational homomorphism. Then f extends uniquely to an algebraic group homomorphism $G \to H$.*

When H is commutative, this lemma is a special case of the next lemma. Indeed, if one takes the G-action on H to be trivial, then the condition in the following lemma is precisely the condition for a map to be a homomorphism.

Lemma 5.2.1.2. *Suppose that G is a connected algebraic group and $(H, +)$ is a commutative algebraic group with an algebraic automorphic G-action ρ. Let $f : G \to H$ be a rational map such that[128] $f(xy) = f(x) + {}^x f(y)$ for all $x, y, xy \in \mathrm{dom}(f)$. Then f extends to an algebraic map satisfying $f(xy) = f(x) + {}^x f(y)$ for all $x, y \in G$.*

Proof. Since f is rational and G is connected, $\mathrm{dom}(f) = U \subseteq G$ is a dense open subset. Set $V = U \cap U^{-1}$.

Fix $x \in V$. Consider the rational map

$$f_x : G \to H, \qquad f_x(y) := f(yx) + {}^{yx} f(x^{-1}).$$

[126] In this thesis, an **algebraic variety** over the field $\mathbb{K}$ is a reduced affine $\mathbb{K}$-scheme which is separated, i.e. the diagonal map is a closed immersion. In particular, since algebraic groups are separated, all algebraic groups are varieties. Furthermore, **algebraic maps** of algebraic varieties are just morphisms of schemes, and **rational maps** are algebraic maps which are only defined on an open dense subset of the domain. See Chapter AG in [Borel, 1991], for example, for more details.

[127] Recall that an open subset of a topological space X is called **dense** if it has non-empty intersection with every non-empty open set of X.

[128] Here we use the notation that ${}^x f(y) := \rho(x)(f(y))$.

This map is rational since it is defined on the dense open set Vx^{-1}. Observe that on $V \cap Vx^{-1}$ we have that $f_x = f$ by the assumption on f. Now, let $x, z \in V$ and define the rational map

$$f_{x,z} : G \to H, \qquad f_{x,z}(y) := f_x(y) - f_z(y).$$

Then $f_{x,z}$ is defined on $Vx^{-1} \cap Vz^{-1}$. If the set $f_{x,z}^{-1}(H\backslash\{0\})$ is non-empty, it is open dense. Hence, it has non-empty intersection with $V \cap Vx^{-1} \cap Vz^{-1}$. However, since on $V \cap Vx^{-1} \cap Vz^{-1}$ we have $f = f_x = f_z$, this is impossible. Thus, we must have $f_{x,z} \equiv 0$ on $Vx^{-1} \cap Vz^{-1}$. In particular, if $y \in Vx^{-1} \cap Vz^{-1}$ then $f_x(y) = f_z(y)$.

Therefore, the following map is a well-defined locally-algebraic, and hence algebraic, map

$$\widehat{f} : G \to H, \qquad \widehat{f}(y) := f_w(y) \ \text{ where } \ w \in y^{-1}V.$$

This map clearly restricts to f on V. Furthermore, it satisfies the condition from the lemma:

Let $a, b \in G$. Choose $w \in b^{-1}a^{-1}V \cap b^{-1}V$ – this exists since both these sets are open dense in G. We then have $abw \in V$ and $bw \in V$. The condition on f tells us that $0 = f(1) = f(bw) + {}^{bw}f(w^{-1}b^{-1})$. Hence, we have the equations

$$\widehat{f}(ab) = f_w(ab) = f(abw) + {}^{abw}f(w^{-1}),$$

$$\widehat{f}(a) = f_{bw}(a) = f(abw) + {}^{abw}f(w^{-1}b^{-1}),$$
$${}^{a}\widehat{f}(b) = {}^{a}f_w(b) = {}^{a}f(bw) + {}^{abw}f(w^{-1}).$$

This then gives us that $\widehat{f}(ab) = \widehat{f}(a) + {}^{a}\widehat{f}(b)$, as required.

□

Recall that a rational[129] representation of an algebraic group G is a vector space V, equipped with an algebraic homomorphism $\theta : G \to \mathrm{GL}(V)$. An immediate consequence of Lemma 5.2.1.1 is that if G is connected, then θ is uniquely determined by any of its restrictions to an open subset and any rational homomorphism of algebraic groups $G \to GL(V)$ determines a representation.

Similar to the case of abstract groups, we have the following proposition. This in fact follows from Proposition 5.1.1.1.

Proposition 5.2.1.3. *[Xanthopoulos, 1992, Section 4.3] Suppose that V is a finite-dimensional indecomposable restricted $\mathfrak{g}$-module, where $\mathfrak{g}$ is the Lie algebra of the algebraic group G over $\mathbb{K}$. Then as algebraic groups we have*

$$\mathrm{Aut}_{\mathfrak{g}}(V) = \mathbb{K}^{\times} \times (1 + J)$$

where J is the Jacobson radical of $\mathrm{End}_{\mathfrak{g}}(V)$*. Furthermore, $1 + J$ is a connected*

[129]It is a standard terminology, which slightly disagrees with our usage of the adjective *rational*.

unipotent algebraic subgroup of $\mathrm{Aut}_{\mathfrak{g}}(V)$*.*

5.2.2 Rational and algebraic cohomologies

Let H be an affine group scheme acting on an additive algebraic group $(A, +)$ algebraically by automorphisms. The following easy lemma shall be useful in what follows.

Lemma 5.2.2.1. *Let H be an irreducible*[130] *affine group scheme. Then H is primary, i.e., every zero-divisor in $\mathbb{K}[H]$ lies inside the nilradical.*

Proof. The affinity of H tells us that $\mathbb{K}[H] = \mathbb{K}[y_1, \ldots, y_n]/I$ for some $n \geqslant 1$ and some Hopf ideal I. In particular, I has a primary decomposition $I = Q_0 \cap \ldots \cap Q_r$ (which we assume to be normal) with associated primes $P_0 = \sqrt{I}, P_1, \ldots, P_r$. From the perspective of group schemes, this uniquely endows H with a finite collection $p_0, p_1, \ldots, p_r$ of embedded points of H, where p_i is a generic point of the irreducible closed subscheme given by Q_i. Furthermore, for $i > 0$ each p_i is of codimension at least one. If x is a closed point in H, then the set $xp_0, xp_1, \ldots, xp_r$ corresponds to the associated primes of another primary decomposition of I. Hence, by uniqueness, x acts on the set $p_0, p_1, \ldots, p_r$ by permutation. Thus, $H_{red} = \bigcup_{i=1}^{r}(\bigcup_{x \text{ closed point}} xp_i)_{red} = \bigcup_{i=1}^{r}(p_i)_{red}$. However, over an algebraically closed field, H_{red} cannot be a finite union of proper subvarieties. Hence, $r = 0$ and the result follows. $\square$

Define the cochain complex $(C^n_{Rat}(H; A), d)$ to consist of the rational maps $H^n \to A$ defined at $(1, 1, \ldots, 1)$ with the standard differentials of group cohomology.

A rational function f on H^n is defined on an open dense subset $U \subseteq H^n$, thus, U has a non-empty intersection $U_\alpha = U \cap H^n_\alpha$ with each irreducible component H^n_α of H^n. Since H^n is a group scheme, its irreducible components are connected components that yields the direct sum decomposition of functions:

$$\mathbb{K}[H^n] = \oplus_\alpha \mathbb{K}[H^n_\alpha].$$

Note that each H_α is isomorphic to an irreducible affine group scheme, so we can apply Lemma 5.2.2.1. Thus, U_α is of the form $U(s_\alpha)$ for a non-zero-divisor $s_\alpha \in \mathbb{K}[H^n_\alpha]$ and $f = hs^{-1}$ for some $h \in \mathbb{K}[H^n]$ and a non-zero-divisor $s := (s_\alpha) \in \mathbb{K}[H^n]$. Thus, $f \in \mathbb{K}[H^n]_S$, the localised ring of functions obtained by inverting the set S of all non-zero-divisors.

Writing functions on the algebraic group A as $\mathbb{K}[A] = \mathbb{K}[x_1, \ldots x_m]/I$, a rational n-cochain μ is uniquely determined by an m-tuple of rational functions $(\mu_i) \in \mathbb{K}[H^n]^m_S$ satisfying the relations of I. In particular, if each component of

[130] A scheme is called **irreducible** if the underlying topological space cannot be written as the union of two proper closed subsets.

H is infinitesimal,

$$\mathbb{K}[H^n]_S = \mathbb{K}[H^n] \quad \text{and} \quad C^n_{Rat}(H;A) = C^n_{Alg}(H;A) \ ,$$

where, in general, $(C^n_{Alg}(H;A), d)$ is the cochain subcomplex of $(C^n_{Rat}(H;A), d)$ that consists of those rational maps $H^n \to A$ which are, in fact, algebraic.

Let us now concentrate on a connected algebraic group G and its connected subgroup scheme L. There is another subcomplex of $(C^n_{Rat}(G;A), d)$ which we are interested in: we define $(\widetilde{C}^\bullet_{Rat}(G, L; A), d)$ to consist of rational maps $G^n \to A$ that are trivial on L^n (i.e., everywhere 0 on L^n). As in the case of abstract groups, we define $(C^\bullet_{Rat}(G, L; A), d)$ by

$$C^n_{Rat}(G, L; A) = \begin{cases} \widetilde{C}^n_{Rat}(G, L; A), & \text{if } n > 0, \\ A^L, & \text{if } n = 0. \end{cases}$$

There is a natural inclusion of cochain complexes $C^\bullet_{Rat}(G, L; A) \to C^\bullet_{Rat}(G; A)$. We can hence define the cochain complex $\widetilde{C}^\bullet_{Rat}(L; A)$ such that $\widetilde{C}^n_{Rat}(L; A) := \operatorname{Coker}(C^n_{Rat}(G, L; A) \to C^n_{Rat}(G; A))$ for all $n \geqslant 0$.

In particular, this gives us the short exact sequence of cochain complexes

$$0 \to C^\bullet_{Rat}(G, L; A) \to C^\bullet_{Rat}(G; A) \to \widetilde{C}^\bullet_{Rat}(L; A) \to 0.$$

We define the algebraic complexes $C^\bullet_{Alg}(G, L; A)$ and $\widetilde{C}^\bullet_{Alg}(L; A)$ in the expected way, and once again get a short exact sequence of cochain complexes. In either case, this allows us to construct the long exact sequence in cohomology (suppressing the 'Rat' and 'Alg'):

$$\begin{aligned} 0 \to H^1(G, L; A) \to H^1(G; A) \to \widetilde{H}^1(L; A) \to \cdots \\ \ldots \to \widetilde{H}^{n-1}(L; A) \to H^n(G, L; A) \to H^n(G; A) \to \widetilde{H}^n(L; A) \to \cdots \end{aligned}$$

Note that $\widetilde{H}^0_{Rat}(L; A) = \widetilde{H}^0_{Alg}(L; A) = 0$, hence this exact sequence starts in degree one.

These long exact sequences can be connected, using the maps induced by the inclusions $C^n_{Alg}(G, L; A) \hookrightarrow C^n_{Rat}(G, L; A)$ and $C^n_{Alg}(G; A) \hookrightarrow C^n_{Rat}(G; A)$:

$$\begin{tikzcd} \cdots \arrow[r] & H^n_{Alg}(G;A) \arrow[r] \arrow[d] & \widetilde{H}^n_{Alg}(L;A) \arrow[r] \arrow[d] & H^{n+1}_{Alg}(G,L;A) \arrow[r] \arrow[d] & \cdots \\ \cdots \arrow[r] & H^n_{Rat}(G;A) \arrow[r] & \widetilde{H}^n_{Rat}(L;A) \arrow[r] & H^{n+1}_{Rat}(G,L;A) \arrow[r] & \cdots . \end{tikzcd}$$

Since we identify $C^0_{Alg}(G; A)$ with algebraic maps from the trivial algebraic group to A (and similarly in the other complexes), there is no distinction between rational and algebraic maps. Hence,

$$H^0_{Rat}(G;A) = H^0_{Alg}(G;A) = H^0_{Rat}(G,L;A) = H^0_{Alg}(G,L;A) = A^G.$$

The cocycle condition on $f \in C^1_{Rat}(G;A)$ is precisely the condition considered in Lemma 5.2.1.2 for a rational map $f : G \to A$. Since G is connected, Lemma 5.2.1.2 tells us the map extends to an algebraic map. Hence, in this case

$$H^1_{Rat}(G;A) = H^1_{Alg}(G;A) \text{ and } H^1_{Rat}(G,L;A) = H^1_{Alg}(G,L;A).$$

This leads to the following proposition. The first part of it follows from the exact sequence. The second part has a similar proof as Proposition 5.1.2.2.

Proposition 5.2.2.2. *(cf. Proposition 5.1.2.2)*

(1) *If $\widetilde{H}^1_{Rat}(L;A) = 0$, then $H^1_{Rat}(G,L;A) = H^1_{Rat}(G;A)$.*

(2) *For $n > 0$, if the natural map $Z^{n-1}_{Rat}(G;A) \to \widetilde{Z}^{n-1}_{Rat}(L;A)$ is surjective, then the natural map $H^n_{Rat}(G,L;A) \to H^n_{Rat}(G;A)$ is injective.*

The appropriate long exact sequence yields the following.

Corollary 5.2.2.3. *The cohomology group $H^2_{Rat}(G,L;A)$ is trivial if and only if $H^1_{Rat}(G;A) \to \widetilde{H}^1_{Rat}(L;A)$ is surjective and $H^2_{Rat}(G;A) \to \widetilde{H}^2_{Rat}(L;A)$ is injective.*

When the action is trivial, we can learn more about what these cohomology groups are.

Lemma 5.2.2.4. *If G acts trivially on A and* $\mathrm{Hom}(L,A) = 0$*, then $\widetilde{Z}^1_{Rat}(L;A) = 0$.*

Proof. Let $\mu + C^1_{Rat}(G,L;A) \in \widetilde{Z}^1_{Rat}(L;A)$, so $d\mu \in C^2_{Rat}(G,L;A)$. In particular, $d\mu|_{L^2} = 0$. However, since the action is trivial, $d\mu|_{L^2} = 0$ if and only if $\mu|_L$ is a rational homomorphism $L \to A$ if and only if $\mu|_L$ is a homomorphism $L \to A$ (since L is connected, by assumption). Since $\mathrm{Hom}(L,A) = 0$, we conclude that $\mu + C^1_{Rat}(G,L;A) = 0 + C^1_{Rat}(G,L;A)$. Hence, $\widetilde{Z}^1_{Rat}(L;A) = 0$. ☐

Lemma 5.2.2.5. *Let G be a connected algebraic group which acts trivially on a commutative algebraic group A. Let $L \leqslant G$ be a closed connected subgroup scheme. Then $H^1_{Rat}(G;A) = \mathrm{Hom}(G,A)$ and $H^1_{Rat}(G,L;A) = \{\mu \in \mathrm{Hom}(G,A) \mid \mu|_L \equiv 0\}$.*

Proof. The coboundary map $C^0_{Rat}(G;A) \to C^1_{Rat}(G;A)$ is just the trivial map since the G-action on A is trivial. Hence, we get that $H^1_{Rat}(G;A) = Z^1_{Rat}(G;A)$, the rational 1-cocycles of G. However, as the action is trivial, rational 1-cocycles of G on A are the same as homomorphisms of algebraic groups $G \to A$. Hence, $H^1_{Rat}(G;A) = \mathrm{Hom}(G,A)$.

Essentially the same argument gives

$$H^1_{Rat}(G,L;A) = \{\mu \in \mathrm{Hom}(G,A) \mid \mu|_L \equiv 0\}.$$

□

Combining Lemma 5.2.2.5 with Lemma 5.2.2.4 and Proposition 5.2.2.2(2), we get the following corollary.

Corollary 5.2.2.6. *Let G be a connected algebraic group acting algebraically (not necessarily trivially) by automorphisms on a commutative algebraic group A. Let $L \leqslant G$ be a connected closed subgroup scheme of G such that the action of L on A is trivial, and* $\mathrm{Hom}(L, A) = 0$. *Then $H^1_{Rat}(G, L; A) = H^1_{Alg}(G; A)$ and $H^2_{Rat}(G, L; A) \to H^2_{Rat}(G; A)$ is injective.*

The following result from [van der Kallen, 1973, Prop. 2.2] is useful in what follows.

Lemma 5.2.2.7. *Let G be a semisimple, simply-connected algebraic group. Suppose further that, if $p = 2$, the Lie algebra $\mathfrak{g}$ of G does not contain A_1, B_2 or C_l ($l \geqslant 3$) as a direct summand. Then $\mathfrak{g}$ is perfect, i.e., $\mathfrak{g} = [\mathfrak{g}, \mathfrak{g}]$.*

Proof. It is enough to prove this result for G simple and simply-connected, with irreducible root system Φ. It is known[131] that $\mathfrak{g}$ is simple and non-abelian (and so $\mathfrak{g} = [\mathfrak{g}, \mathfrak{g}]$) in the following cases: $p \nmid l + 1$ in type A_l, $p \neq 2$ in types B_l, C_l, D_l, E_7 and F_4, $p \neq 3$ in types E_6 and G_2, and arbitrary p in type E_8.

Furthermore, we obtain from Table 1 in [Hogeweij, 1982] that $\mathfrak{g} = [\mathfrak{g}, \mathfrak{g}]$ in all the remaining cases except for $p = 2$ in types A_1, B_2, C_l ($l \geqslant 3$). □

Lemma 5.2.2.8. *Let G be a semisimple, simply-connected algebraic group over an algebraically closed field $\mathbb{K}$ of characteristic p which acts trivially on a commutative algebraic group A. Suppose further that, if $p = 2$, the Lie algebra $\mathfrak{g}$ of G does not contain A_1, B_2 or C_l ($l \geqslant 3$) as a direct summand. Let G_1 be the first Frobenius kernel of G. Then $H^2_{Rat}(G, G_1; A) = 0$.*

Proof. Let us first show that $H^2_{Rat}(G; A) = 0$. Let $\mu : G \times G \to A$ be a rational cocycle defined on the open set $U \times U$ with $U^{-1} = U$. We can define a local group structure on the set $A \times G$ by setting

$$(a, g)(b, h) = (a + b + \mu(g, h), gh) \ \text{ and } \ (a, g)^{-1} = (-a - \mu(g, g^{-1}), g^{-1}).$$

In the language of [Weil, 1955], $A \times U$ is a group-chunk in the pre-group $A \times G$. By Weil's theorem,[132] there exists an algebraic group H birationally equivalent to $A \times U$ with $\Phi : A \times U \to \Phi(A \times U)$ an isomorphism of algebraic group-chunks and $\Phi(A \times U)$ a dense open set in H.

Since H is connected it is generated by $\Phi(A \times U)$. Let $f : A \to H$ be the natural algebraic group homomorphism coming from $A \to A \times U$. This is clearly injective and, since A commutes with each element of $A \times U$, we have $f(A) \subseteq Z(H)$.

[131]See, for example, Corollary 2.7 in [Hogeweij, 1982].
[132]See [Weil, 1955].

Furthermore, the natural projection $A \times U \to G$ extends to a rational (and so algebraic) homomorphism $\pi : H \to G$, which is surjective as U generates G (since G connected). Finally, it is clear that $f(A) = \ker \pi \cap \Phi(A \times U)$. Hence, π descends to a homomorphism $\bar{\pi} : H/f(A) \to G$, whose kernel is discrete (since $\Phi(A \times U)$ is dense in H) and, hence, central (as G connected).

In other words, we have a central extension $1 \to A \to H \to G \to 1$ of algebraic groups, which corresponds to an algebraic cocycle $\widetilde{\mu} : G \times G \to A$. It is straightforward to see that $\widetilde{\mu}|_{U \times U} = \mu|_{U \times U}$, and hence $[\mu]$ lies in the image of the natural map $H^2_{Alg}(G; A) \to H^2_{Rat}(G; A)$. Therefore, the map $H^2_{Alg}(G; A) \to H^2_{Rat}(G; A)$ is surjective.

It suffices to prove that $H^2_{Alg}(G; A) = 0$ when A is $\mathbb{G}_a$ or $\mathbb{G}_m$ or a finite group: the long exact sequence in cohomology reduces the case of arbitrary A to one of these cases. It is known[133] that $H^2_{Alg}(G; \mathbb{G}_a) = H^2(G; \mathbb{K}_{triv}) = 0$.

Consider a non-trivial cohomology class in $H^2_{Alg}(G; A)$ when A is $\mathbb{G}_m$ or a non-trivial finite group. It yields a non-split central extension $1 \to A \to \widetilde{G} \to G \to 1$. Pick a non-trivial character $\chi : A \to \mathbb{G}_m$. There exists an irreducible representation of $\widetilde{G}$ with a central character χ. It is an irreducible projective representation[134] of G. By the original version of Steinberg's tensor product theorem[135] it is linear. Hence, χ is trivial. This contradiction proves that $H^2_{Alg}(G; A) = 0$ for these two particular A. We have finished the proof that $H^2_{Rat}(G; A) = 0$ for an arbitrary A.

Since G_1 is a height 1 group scheme, rational homomorphisms of schemes $G_1 \to A$ are fully controlled by the corresponding restricted homomorphisms of Lie algebras $\mathfrak{g} \to \mathrm{Lie}(A)$. By Lemma 5.2.2.7, $\mathfrak{g} = [\mathfrak{g}, \mathfrak{g}]$ and thus all such homomorphism of Lie algebras are trivial. Hence, we can apply Corollary 5.2.2.6 to get that $H^2_{Rat}(G, G_1; A) \to H^2_{Rat}(G; A)$ is injective, and so $H^2_{Rat}(G, G_1; A) = 0$. □

5.2.3 G-Stable bricks

In Section 5.1, we have introduced the notions of weak (L, H)-morphs and (L, H)-morphs for abstract groups. In this subsection, we discuss how these notions apply to algebraic groups and see how they can be used to shed some light on the lifting of $\mathfrak{g}$-modules to G-modules.

Suppose that G, K are algebraic groups over $\mathbb{K}$, where G is connected, and that L, H are closed subgroup schemes of G, K respectively. We say that a rational map $f : G \to K$ is *a (weak) (L, H)-morph of algebraic groups* if it satisfies the conditions for a (weak) (L, H)-morph of abstract groups given in Subsection 5.1.2, where the condition (M3) is interpreted for only those $x, y, xy \in \mathrm{dom}(f)$.

In analogy with the case of abstract groups, a weak (L, H)-morph of algebraic groups is a homomorphism $G \to N/H$ with a rational lifting $N/H \to N$ which

[133] See Section II.4.11 in [Jantzen, 1987].

[134] A **projective representation** of G is a pair (V, θ) where V is a $\mathbb{K}$-vector space and $\theta : G \to \mathrm{PGL}(V)$ is a homomorphism of algebraic groups.

[135] See [Steinberg, 1963].

satisfies an additional condition. It is clear that if H is normal in K then condition (M2) is trivially satisfied. We again have that weak $(L,1)$-morphs are just homomorphisms $G \to K$, and that weak $(1,K)$-morphs are rational maps $G \to K$ which preserve the identity.

We say that two weak (L,H)-morphs of algebraic groups, f and g, are equivalent if $f(x)g(x)^{-1} \in H$ for all $x \in \mathrm{dom}(f) \cap \mathrm{dom}(g)$. Given a homomorphism of algebraic groups $\theta : L \to K$, we denote by $[LH]^{\theta}\mathrm{mo}(G,K)$ the quotient by this equivalence relation of the set of weak (L,H)-morphs of algebraic groups from G to K which restrict to θ on L. The reader may note that the notation here is the same as the notation for abstract groups, but, since we only deal with algebraic groups for the remainder of the chapter, no confusion should arise.

Suppose that X is a separated algebraic scheme on which G acts rationally on the right (i.e. the action $X \times G \to X$ is a rational map), K acts algebraically on the left, and the actions commute. Suppose further that $\theta \in X(\mathbb{K})$ is such that $\theta^G \subseteq {}^K\theta$, and that there exists a rational section $K/H \to K$ where $H = \mathrm{Stab}_K(\theta)$ is the scheme-theoretic stabiliser of θ.

As in the case for abstract groups, this gives us a rational map

$$f : G \to K \quad \text{characterised by} \quad {}^{f(x)}\theta = \theta^x \quad \text{for all } x \in U \overset{open}{\subseteq} G.$$

Lemma 5.2.3.1. *The map f defined above is a $(1,H)$-morph of algebraic groups.*

Proof. We can think of f as the composition of the following rational maps

$$G \hookrightarrow \{\theta\} \times G \to {}^K\theta \to K/H \to K.$$

Note that Proposition 3.2.1 in [Demazure and Gabriel, 1970] precisely says that ${}^K\theta \to K/H$ is an algebraic map. We then have that the composition is rational since each domain of definition intersects the previous map's image.

The proof that $f(x)f(y) \in f(xy)H$ for $x, y \in G$ with $f(x), f(y)$ and $f(xy)$ defined is exactly the same as in the abstract case, as is the proof that $f(G) \subseteq N_K(H)$.

□

Now we fix algebraic (group, subgroup scheme) pairs (G,L) and (K,H) with H soluble and G connected. Denote by m_G, m_K the corresponding multiplication maps, Δ_G, Δ_K the diagonal embeddings, and inv_G, inv_K the inverse maps. Let $\theta : L \to K$ be a homomorphism of algebraic group schemes. Furthermore, choose $\widetilde{H}$ to be an algebraic subgroup of H, characteristic in $N = N_K(H)$ such that $A := H/\widetilde{H}$ is commutative. We denote the quotient map $H \to A$ by π.

We can define an N-action on H by conjugation. Note that since $\widetilde{H}$ is characteristic in N, so preserved by conjugation, this passes to an algebraic N-action on A. Hence, we have an algebraic action of N on A which is trivial on H (since A is commutative). This gives us an algebraic N/H-action on A. For an element

$f \in [LH]^\theta \mathrm{mo}(G,K)$, we get a rational homomorphism $G \to N/H$ which is, in fact, algebraic by Lemma 5.2.1.1. Thus, every element of $[LH]^\theta \mathrm{mo}(G,K)$ induces an algebraic G-action on A. This G-action respects the multiplication operation of A, i.e. it is an algebraic automorphic G-action.

As in the case for abstract groups, we can form something resembling an exact sequence. Let ρ be a rational G-action on A, and define

$$[L\widetilde{H}]^\theta \mathrm{mo}(G,N)_\rho \subseteq [L\widetilde{H}]^\theta \mathrm{mo}(G,N), \qquad [LH]^\theta \mathrm{mo}(G,N)_\rho \subseteq [LH]^\theta \mathrm{mo}(G,N)$$

as the subsets of weak morphs which induce the action ρ.

We get the following theorem.

Theorem 5.2.3.2. *(cf. Theorem 5.1.2.4) For a rational G-action ρ on A the following statements hold:*

(1) *There is a restriction map*

$$\mathrm{Res} : [L\widetilde{H}]^\theta \mathrm{mo}(G,N)_\rho \longrightarrow [LH]^\theta \mathrm{mo}(G,N)_\rho, \quad \mathrm{Res}(\langle f \rangle) = [f]$$

where $\langle f \rangle$ and $[f]$ denote the equivalence classes in $[L\widetilde{H}]^\theta \mathrm{mo}(G,N)_\rho$ and $[LH]^\theta \mathrm{mo}(G,N)_\rho$.

(2) *The abelian group $Z^1_{Rat}(G,L;(A,\rho))$ acts freely on the set $[L\widetilde{H}]^\theta \mathrm{mo}(G,N)_\rho$ by*

$$\gamma \cdot \langle f \rangle := \langle \dot{\gamma} f \rangle \quad \textit{where} \quad \dot{\gamma} f = m_K \circ (\dot{\gamma} \times f) \circ \Delta_G$$

and $\dot{\gamma} : G \xrightarrow{\gamma} A \to H$ comes from a rational Rosenlicht section $A \to H$ (cf. [Rosenlicht, 1956, Theorem 10]) with $\dot{\gamma}(1) = 1$.

(3) *The corestricted restriction map* $\mathrm{Res} : [L\widetilde{H}]^\theta \mathrm{mo}(G,N)_\rho \longrightarrow \mathrm{Im}(\mathrm{Res})$ *is a quotient map by the $Z^1_{Rat}(G,L;(A,\rho))$-action.*

(4) *If H, $\widetilde{H}$ and A are reduced, two classes $\langle f \rangle, \langle g \rangle \in [L\widetilde{H}]^\theta \mathrm{mo}(G,N)_\rho$ lie in the same $B^1_{Rat}(G,L;(A,\rho))$-orbit if and only if there exist $h \in H$, $f' \in \langle f \rangle$, $g' \in \langle g \rangle$ such that $[f(L),h] \subseteq \widetilde{H}$ and $f'(x) = hg'(x)h^{-1}$ for all $x \in G$.*

(5) *There is an obstruction map*

$$\mathrm{Obs} : [LH]^\theta \mathrm{mo}(G,N)_\rho \longrightarrow H^2_{Rat}(G,L;(A,\rho)), \quad \mathrm{Obs}([f]) = [f^\sharp]$$

where the cocycle $f^\sharp$ is defined by

$$G \times G \xrightarrow{(p_1,p_2,m_K)} G \times G \times G \xrightarrow{(f,f,inv_K f)} K \times K \times K \xrightarrow{m_K} H \xrightarrow{\pi} A$$

Here, p_1 and p_2 denote projection to the first and second coordinate respectively.

(6) *The sequence (cf. Sequence (5.1))*

$$[L\widetilde{H}]^{\theta}\mathrm{mo}(G,N)_{\rho} \longrightarrow [LH]^{\theta}\mathrm{mo}(G,N)_{\rho} \longrightarrow H^2_{Rat}(G,L;(A,\rho))$$

is exact, i.e., the image of Res *is equal to* $\mathrm{Obs}^{-1}([0])$.

Proof. If $\langle f\rangle = \langle g\rangle$ then the map

$$\alpha : G \xrightarrow{(f,inv_K g)} K \times K \xrightarrow{m} K$$

has image in $\widetilde{H}$ and is trivial on L. It is rational as it is a composition of rational maps, and the identity is in the domain of definition and image of each map.

We also observe that given an analogous $\alpha : G \to H$ (i.e. corresponding to $[f] = [g]$) we get $\pi\alpha : G \to A$. Denoting the Rosenlicht section[136] $A \to H$ by τ, we see that $\tau\pi\alpha = \alpha$ and thus $\dot{(\pi\alpha)} = \alpha$. Note that we may assume that the Rosenlicht section is defined at 0_A by composing with a translation if necessary. All the maps here are rational. In particular, $\pi\alpha \in C^1_{Rat}(G,L;(A,\rho))$.

With these observations in mind, the remainder of the proof follows in the same way as in the proof of Theorem 5.1.2.4 does for abstract groups, doing everything diagrammatically.

□

Before going any further, let's consider the following case where we can use this exact sequence directly. A restricted $\mathfrak{g}$-module (V,θ) satisfying the condition that $\mathrm{Aut}_{\mathfrak{g}}(V) = \mathbb{K}^{\times}$ is called a **brick**. A brick is necessarily an indecomposable $\mathfrak{g}$-module.

Theorem 5.2.3.3. *Suppose G is a semisimple, simply-connected algebraic group over an algebraically closed field $\mathbb{K}$ of characteristic $p > 0$, with Lie algebra $\mathfrak{g}$. Suppose further that, if $p = 2$, the Lie algebra $\mathfrak{g}$ does not contain A_1, B_2 or C_l ($l \geqslant 3$) as a direct summand. Let (V,θ) be a finite-dimensional G-stable brick. Then there exists a unique G-module structure Θ on V with $\Theta|_{G_1} = \theta$.*

Proof. We use Theorem 5.2.3.2 in the following situation:

- $L = G_1$, the first Frobenius kernel of G.
- $K = \mathrm{GL}(V)$.
- $H = \mathrm{Aut}_{\mathfrak{g}}(V) = \mathbb{K}^{\times}$.
- $N = N_K(H)$.
- $X = \mathrm{Hom}_{\mathbb{K}}(\mathfrak{g}, \mathfrak{gl}(V))$, a separated affine scheme with $\theta \in X(\mathbb{K})$.

[136] See [Rosenlicht, 1956, Theorem 10].

Observe that G acts on X on the right via the adjoint map on the domain and $\mathrm{GL}(V)$ acts on X on the left via conjugation on the image. Furthermore, the actions commute, and the G-stability of V gives us that $\theta^G \subseteq {}^{\mathrm{GL}(V)}\theta$.

Hence, Lemma 5.2.3.1 gives us a $(1, H)$-morph of algebraic groups, which we denote $f : G \to \mathrm{GL}(V)$. In particular, it gives a homomorphism of algebraic groups $f : G \to \mathrm{PGL}(V)$, together with a rational lifting $\eta : \mathrm{PGL}(V) \to \mathrm{GL}(V)$. This rational lifting can be defined as follows: fix a basis of V and let U be the open subset of $\mathrm{PGL}(V)$ consisting of all cosets which can be represented by a (unique) matrix $A = (a_{ij}) \in \mathrm{GL}(V)$ with $a_{11} = 1$. Then define the map $\eta : U \to \mathrm{GL}(V)$ by assigning to each coset this representative.

Currently f and θ give the same maps from G_1 to N/H – since

$$^{\theta(x)}\theta(a)(v) = \theta(x)\theta(a)\theta(x^{-1})(v) = \theta(xax^{-1})(v) = \theta^x(a)(v)$$

for $x, a \in G_1(\mathbb{S})$, $v \in V(\mathbb{S})$ for any commutative $\mathbb{K}$-algebra $\mathbb{S}$. Note, however, that the maps $G_1 \to K$ do not necessarily agree.

To fix this potential disagreement, we define a rational map $R : G_1 \to H = \mathbb{K}^\times$ by $R(g) = f(g)^{-1}\theta(g)$ for $g \in G_1(\mathbb{S})$. There exists a rational map $\widetilde{R} : G \to H = \mathbb{K}^\times$ which restricts to R on G_1. Indeed, we have $R \in \mathbb{K}[G_1]$ (as G_1 is infinitesimal), so we can lift it to $\widetilde{R} \in \mathbb{K}[G]$ (since $\mathbb{K}[L]$ is a quotient of $\mathbb{K}[G]$). Let $U = G \backslash \widetilde{f}^{-1}(0)$. This is open in G, and on U we have that the image of $\widetilde{R}$ lies inside $\mathbb{K}^\times$, so $\widetilde{R}$ is a rational map $G \to \mathbb{K}^\times$. If now we define $\widetilde{f} : G \to \mathrm{GL}(V)$ by $\widetilde{f}(g) = f(g)\widetilde{R}(g)$, we get that $\widetilde{f}$ is a (G_1, H)-morph which restricts to θ on G_1, fixing the disagreement.

Observe that with $\widetilde{H} := 1$, we get (in the notation of the Theorem 5.2.3.2) $A = H$ and G acting on A trivially. Hence, the "exact sequence" from Theorem 5.2.3.2 is

$$H^1_{Rat}(G, G_1; \mathbb{K}^\times) \dashrightarrow [G_1 1]^\theta \mathrm{mo}(G, N)_1 \to [G_1 H]^\theta \mathrm{mo}(G, N)_1 \to H^2_{Rat}(G, G_1; \mathbb{K}^\times)$$

By Lemma 5.2.2.8, $H^2_{Rat}(G, G_1; \mathbb{K}^\times) = 0$. Hence $[\widetilde{f}] \in [G_1 H]^\theta \mathrm{mo}(G, N)_1$ can be lifted to $\widehat{f} \in [G_1 1]^\theta \mathrm{mo}(G, N)_1$. This means that $\Theta := \widehat{f} : G \to \mathrm{GL}(V)$ is a homomorphism of algebraic groups which restricts to θ on G_1. Furthermore, this representation is unique (up to equivalence) if $H^1_{Rat}(G, G_1; \mathbb{K}^\times) = 0$.

By Lemma 5.2.2.5, $H^1_{Rat}(G, G_1; \mathbb{K}^\times) = \{\mu \in \mathrm{Hom}(G; \mathbb{K}^\times) \mid \mu|_{G_1} \equiv 1\}$. Since G is perfect, $H^1_{Rat}(G, G_1; \mathbb{K}^\times) = 0$ and the extension is unique. □

We recall from Remark 8 that irreducible G_1-modules can be extended to G-modules when G is a semisimple, simply-connected algebraic group. Since irreducible $U_0(\mathfrak{g})$-modules are clearly bricks and Proposition II.3.11 in [Jantzen, 1987] shows that they are G-stable, this theorem provides another approach to that result. This approach is similar to the one used in Theorem 1 of [Cline, Parshall and Scott, 1980] to show the same thing, which also involves lifting a projective representation $G \to \mathrm{PGL}(V)$ to a representation $G \to \mathrm{GL}(V)$. In that result, the projective representation is obtained from the structure theory of semisimple algebras and the lifting comes from the simply-connectedness of G. As in the proof of Theorem 5.2.3.3, much of the proof in [Cline, Parshall and Scott, 1980] involves showing that the lifted representation indeed extends the $\mathfrak{g}$-module structure. This proves to be one of the main complications in adapting our method from abstract groups to algebraic groups, as we shall further see in Subsection 5.2.4.

5.2.4 G-Stable modules with soluble automorphisms

We return to the general situation, where $(G, L), (K, H)$ are algebraic (group, subgroup scheme) pairs with H soluble, G connected, and H reduced. However, from now on we suppose that L is a normal subgroup scheme of G. We also fix a homomorphism of algebraic groups $\theta : L \to K$, where the image commutes with H, so we are now dealing with (L, H)-morphs. Everything in the previous section can be reformulated in terms of (L, H)-morphs without difficulty - the key difference is that the G-action on A is now trivial on L. Since H is soluble, we can find a subnormal series $H = H_0 \rhd H_1 \rhd \ldots \rhd H_k = \{1\}$ with commutative quotients $A_j = H_{j-1}/H_j$ and each H_j characteristic in $N = N_K(H)$ and reduced.

Suppose that f is an (L, H)-morph of algebraic groups such that $f|_L = \theta$. As in the case of abstract groups, we get the following theorem – it generalises the procedure which we have used for bricks in the previous subsection.

Theorem 5.2.4.1. *(cf. Theorem 5.1.3.1) Given an (L, H)-morph of algebraic groups $f = f_0$ with $f|_L = \theta$, we obtain any $(L, 1)$-morph extending θ by applying the following procedure. Step m is the following:*

(1) *The (L, H_{m-1})-morph $f_{m-1} : G \to N$ such that $f_{m-1}|_L = \theta$ determines a rational G-action ρ_m on A_m.*

(2) *If $\mathrm{Obs}([f_{m-1}]) \neq 0 \in H^2_{Rat}(G, L; (A_m, \rho_m))$, then this branch of the process terminates.*

(3) *If $\mathrm{Obs}([f_{m-1}]) = 0 \in H^2_{Rat}(G, L; (A_m, \rho_m))$, then we choose an (L, H_m)-morph $f_m : G \to N$ such that $\mathrm{Res}([f_m]) = [f_{m-1}]$.*

(4) *For each element of $H^1_{Rat}(G, L; (A_m, \rho_m))$ we choose a different f_m branching the process. (The choices different by an element of $B^1_{Rat}(G, L; (A_m, \rho_m))$ are conjugate by an element of H.)*

(5) *We change m to $m + 1$ and go to step (1).*

An $(L, 1)$-morph which restricts to θ on L is equivalent to f_k for one of the non-terminated branches. Two $(L, 1)$-morphs f, g come from different branches if and only if there is no $h \in H$ such that $f(x) = hg(x)h^{-1}$ for all $x \in G$.

We get the following corollaries, similarly to Subsection 5.1.3:

Corollary 5.2.4.2. *Suppose $H^2_{Rat}(G, L; (A_m, \rho_m)) = 0$ for all m for one of the branches. Then this branch does not terminate and there exists a homomorphism $f : G \to K$ which restricts to θ on L.*

Corollary 5.2.4.3. *Suppose $H^1_{Rat}(G, L; (A_m, \rho_m)) = 0$ for all m for one of the non-terminating branches. Then this branch is the only branch. Moreover, if a homomorphism of algebraic groups $f : G \to K$ restricting to θ exists, then it is unique up to conjugation by an element of H.*

Corollary 5.2.4.4. *Suppose $H^1_{Rat}(G, L; (A_k, \rho_k)) \neq 0$ for one of the non-terminating branches. Then there exist algebraic homomorphisms $G \to K$ which are not conjugate by an element of H.*

We apply this theorem (and these corollaries) in the following case - a generalisation of the case from the previous subsection:

- G is a connected algebraic group over $\mathbb{K}$ with Lie algebra $\mathfrak{g}$.
- $L = G_1$.
- $K = \mathrm{GL}(V)$, where (V, θ) is a finite-dimensional G-stable indecomposable $\mathfrak{g}$-module.
- $H = \mathrm{Aut}_{\mathfrak{g}}(V)$,.
- $X = \mathrm{Hom}_{\mathbb{K}}(\mathfrak{g}, \mathfrak{gl}(V))$, a separated affine scheme with $\theta \in X(\mathbb{K})$.

Applying exactly the same argument as in Theorem 5.2.3.3, we only start to encounter problems when trying to extend the rational map $R : G_1 \to H$ to a rational map on the whole of G. This can be fixed without much difficulty.

As a variety, we have that $H = \mathbb{K}^\times \times \mathbb{K}^n \subseteq \mathbb{K}^{n+1}$ for some n.[137] Hence, we get $R = (R_0, R_1, \ldots, R_n)$ where $R_i \in \mathbb{K}[G_1]$ for $i = 0, 1, \ldots, n$. We can then lift each of these to elements of $\mathbb{K}[G]$, so we obtain $\widetilde{R} = (\widetilde{R_0}, \widetilde{R_1} \ldots, \widetilde{R_n}) : G \to \mathbb{K}^{n+1}$. We would like the image to lie in H. Thus, we define $U = G \backslash R_0^{-1}(0)$. This is an open set in G, so we can view $\widetilde{R}$ as a rational map from G to $\mathbb{K}^\times \times \mathbb{K}^n = H$ which is defined on U, and restricts to R on G_1.

Now we can define $\widetilde{f} : G \to \mathrm{GL}(V)$ as $\widetilde{f}(g) = f(g)\widetilde{R}(g)$. This is a (G_1, H)-morph of algebraic groups, which restricts to θ on G_1. Hence, we are in the situation of Theorem 5.2.4.1. Observe that $\theta : G_1 \to \mathrm{GL}(V)$ extends to a homomorphism of algebraic groups $\Theta : G \to \mathrm{GL}(V)$ if and only if there exists a $(G_1, 1)$-morph of algebraic groups extending θ. In particular, the corollaries to Theorem 5.2.4.1 can be used to determine the existence and uniqueness of a G-module structure on V.

[137] See Proposition 5.2.1.3.

Corollary 5.2.4.5. (Existence Test) *Suppose that G is a connected algebraic group over $\mathbb{K}$ with Lie algebra $\mathfrak{g}$, and suppose further that V is an indecomposable G-stable finite-dimensional $\mathfrak{g}$-module. Then there exists a G-action on V, which respects the $\mathfrak{g}$-module structure, if and only if there is a branch (in the terminology of Theorem 5.2.4.1) which does not terminate; for instance, a branch such that $H^2_{Rat}(G, G_1; (A_m, \rho_m)) = 0$ for all (A_m, ρ_m) on that branch.*

Corollary 5.2.4.6. (Uniqueness Test) *Suppose that G is a connected algebraic group over $\mathbb{K}$ with Lie algebra $\mathfrak{g}$, and that V is an indecomposable G-stable finite-dimensional $\mathfrak{g}$-module. Suppose further that there exists a G-action on V which extends the $\mathfrak{g}$-module structure. This G-action is unique (up to isomorphism) if and only if there is a branch (in the terminology of Theorem 5.2.4.1) such that $H^1_{Rat}(G, G_1; (A_m, \rho_m)) = 0$ for all (A_m, ρ_m) on that branch.*

Observe that combining Corollary 5.2.4.6 with Corollary 5.2.2.6 for the N-stable subnormal series $H_m = 1 + J^m$, $m \geqslant 1$, we get a similar result to Proposition 4.3.1 in [Xanthopoulos, 1992].

5.2.5 Comparison with $C^\bullet_{Rat}(G/L; A)$

Let us now mimic the approach we took in Subsection 5.1.5 and examine how our cochain complex $(C^\bullet_{Rat}(G, L; A), d)$ compares with the complex $(C^\bullet_{Rat}(G/L; A), d)$ on the level of cohomology. We use the notation of Subsection 5.2.3. As with our discussion in Subsection 5.1.5 we have to assume that L acts trivially on A for this discussion to be meaningful – a condition which holds in the examples considered.

Similar to the case for abstract groups, we have the following proposition.

Proposition 5.2.5.1. *Under the aforementioned conditions we have isomorphisms of groups $H^0_{Alg}(G, L; A) \cong H^0_{Alg}(G/L; A)$ and $H^1_{Alg}(G, L; A) \cong H^1_{Alg}(G/L; A)$.*

Proof. Making use of the universal property of the quotient for algebraic groups, the proof follows word-for-word as in Proposition 5.1.5.1. □

Recalling the observation that there is no distinction between H^i_{Alg} and H^i_{Rat} for $i = 0, 1$ this tells us that $H^0_{Rat}(G, L; A) \cong H^0_{Alg}(G/L; A)$ and $H^1_{Rat}(G, L; A) \cong H^1_{Alg}(G/L; A)$ in these circumstances.

The universal property of the quotient for algebraic groups further yields an analogue of Proposition 5.1.5.2.

Proposition 5.2.5.2. *The map $\mathrm{Inf}_{Alg} : H^2_{Alg}(G/L; A) \to H^2_{Alg}(G, L; A)$ and the map $\mathrm{Inf}_{Rat} : H^2_{Rat}(G/L; A) \to H^2_{Rat}(G, L; A)$ are injective.*

Proof. The proof follows as in Proposition 5.1.5.2. □

In the case of abstract groups, Subsection 5.1.5 shows that by making careful choices of (L, H)-morphs in Theorem 5.1.3.1 we can guarantee that the image of the obstruction maps Obs : $[LH]^{\theta}\mathrm{mo}(G,N)_{\rho_i} \longrightarrow H^2(G,L;(A_i,\rho_i))$ always lies inside $H^2(G/L;(A_i,\rho_i)) \hookrightarrow H^2(G,L;(A_i,\rho_i))$. As such, it is possible to reinterpret Theorem 5.1.3.1 using the complex $(C^\bullet(G/L;A),d)$ instead of $(C^\bullet(G,L;A),d)$ at all points. This conclusion for abstract groups, however, relies on the observation that it is always possible to assume that the (L,H)-morphs being considered are normalised. When translating the results to the case of algebraic groups it is far from clear that the analogues of Lemma 5.1.5.3 and Corollary 5.1.5.4 hold.

Question: Can the (L,H)-morphs considered in Subsections 5.2.3 and 5.2.4 be chosen to be normalised?

Chapter 6

Integration of Modules - Exponentials

The approach to the Humphreys-Verma conjecture in Chapter 5 resolves the conjecture if the vanishing of certain cocycles in certain cohomology groups is known. Unfortunately, this requirement creates practical limits on providing a definitive answer to the question, since in many cases these cocycles and cohomology groups are not well understood. As a result, there remains interest in other approaches to the Humphreys-Verma conjecture, and this chapter provides another such example.

6.1 Over-restriction

6.1.1 Over-restricted representations

Let $\mathfrak{g}$ be a restricted Lie algebra over an algebraically closed field $\mathbb{K}$ of characteristic $p > 0$,[138] with p-th power map ${}^{[p]} : \mathfrak{g} \to \mathfrak{g}$. As usual, denote by $U_0(\mathfrak{g})$ its restricted enveloping algebra, and let (V, θ) be a restricted representation.[139] Let $N_p(\mathfrak{g})$ be the p-nilpotent cone of $\mathfrak{g}$, i.e., the set of all $x \in \mathfrak{g}$ such that $x^{[p]} = 0$. Notice that for $x \in N_p(\mathfrak{g})$ we have $\theta(x)^p = \theta(x^{[p]}) = 0$. This allows us to define exponentials for each $x \in N_p(\mathfrak{g})$:

$$e^{\theta(x)} = \sum_{k=0}^{p-1} \frac{1}{k!}\theta(x)^k \in \mathfrak{gl}(V) \ .$$

The element $e^{\theta(x)}$ is invertible because $(e^{\theta(x)})^{-1} = e^{\theta(-x)}$. We define **a pseudo-Chevalley group** G_V as the subgroup of $\mathrm{GL}(V)$ generated by all exponentials $e^{\theta(x)}$ for all $x \in N_p(\mathfrak{g})$.

Proposition 6.1.1.1. *The following statements hold for any finite-dimensional restricted representation* (V, θ) *of* $\mathfrak{g}$*:*

(1) G_V *is a (Zariski) closed subgroup of* $\mathrm{GL}(V)$*.*

[138] In fact, up until Theorem 6.1.1.5, the results hold for an arbitrary field of positive characteristic.

[139] Recall that this means $\theta(x^{[p]}) = \theta(x)^p$ for all $x \in \mathfrak{g}$.

(2) *One can choose finitely many $x_1, x_2 \dots x_n \in N_p(\mathfrak{g})$ such that the following map f is surjective:*

$$f : \mathbb{K}^n \to G_V, \quad f(a_1, a_2, \dots, a_n) = e^{\theta(a_1 x_1)} \cdots e^{\theta(a_n x_n)} .$$

Proof. Proposition I.2.2 in [Borel, 1991] states the following. Consider a family of morphisms $\{f_i : V_i \to G\}_{i \in I}$, where the V_i are irreducible varieties and G is an algebraic group, which satisfies the property that each $f_i(V_i)$ contains the identity of G. Then the group closure $\mathcal{A}(M)$ of $M := \bigcup_{i \in I} f_i(V_i)$ is a connected subgroup of G and there exists a finite sequence $i_1, \dots, i_n$ of elements in I such that $\mathcal{A} = f_{i_1}(V_{i_1})^{e_1} \dots f_{i_n}(V_{i_n})^{e_n}$, where the e_j lie in $\{-1, 1\}$.

Choosing $I = N_p(\mathfrak{g})$, $V_x = \mathbb{K}$, and $f_x(a) = e^{\theta(ax)}$, the results follow. Specifically, we obtain that $\mathcal{A}(\bigcup_{x \in N_p(\mathfrak{g})} f_x(V_x)) = \mathcal{A}(G_V) = \overline{G_V}$ is a closed connected subgroup of $\mathrm{GL}(V)$ and that there exist $x_1, \dots, x_n \in N_p(\mathfrak{g})$ such that $\overline{G_V} = e^{\theta(\mathbb{K}x_1)} \dots e^{\theta(\mathbb{K}x_n)}$. This shows that $\overline{G_V} \subseteq G_V$ and thus that G_V is closed. □

Two particular pseudo-Chevalley groups are worth separate discussion. Let $(U_0(\mathfrak{g}), \theta)$ be the left regular representation of $\mathfrak{g}$ on its restricted enveloping algebra.[140] The exponential $e^{\theta(x)}$ is uniquely determined by its application to the identity

$$e^{\theta(x)}(1) = \sum_{k=0}^{p-1} \frac{1}{k!} x^k \in U_0(\mathfrak{g}) .$$

This element should be called $e^x \in U_0(\mathfrak{g})$. We can identify $e^{\theta(x)}$ with e^x because $G_{U_0(\mathfrak{g})}$ is a subgroup of $\mathrm{GL}_1(U_0(\mathfrak{g}))$ that, in turn, acts on $U_0(\mathfrak{g})$ by left multiplication:

$$G_{U_0(\mathfrak{g})} \leqslant \mathrm{GL}_1(U_0(\mathfrak{g})) \leqslant \mathrm{GL}(U_0(\mathfrak{g})).$$

The element e^x is not group-like in $U_0(\mathfrak{g})$, yet it is close to it in the sense that

$$\Delta(e^x) = e^x \otimes e^x + \mathcal{O}(x^{\lfloor (p+1)/2 \rfloor})$$

where $\mathcal{O}(x^m)$ denotes a sum of terms x^k with $k \geqslant m$. To make this precise, we say that a $U_0(\mathfrak{g})$-module V is **over-restricted** if $\theta(x)^{\lfloor (p+1)/2 \rfloor} = 0$ for all $x \in N_p(\mathfrak{g})$. See Subsection 6.2.2, *infra*, for some examples. Notice that if $p = 2$, then $\lfloor (p+1)/2 \rfloor = 1$ and this requirement is severe: $\theta(x) = 0$.

The second vital example of a pseudo-Chevalley group is $G_{\mathfrak{g}}$, procured from the adjoint representation $(\mathfrak{g}, ad)$.[141] This group is intricately connected with the pseudo-Chevalley groups of over-restricted representations, as the following propositions show.

[140] In other words, we take $V = U_0(\mathfrak{g})$ and for each $w \in U_0(\mathfrak{g})$ we define $\theta(w)$ to be left multiplication by w.

[141] This is a restricted representation of $\mathfrak{g}$.

Proposition 6.1.1.2. *Let $(\mathfrak{g}, ad)$ be the adjoint representation of $\mathfrak{g}$. If (V,θ) is an over-restricted representation of $U_0(\mathfrak{g})$, then*

$$\theta(e^{ad(x)}(y)) = e^{\theta(x)}\theta(y)e^{-\theta(x)}$$

for all $x \in N_p(\mathfrak{g})$, $y \in \mathfrak{g}$.

Proof. First, observe by induction that, for each $k = 1, 2, \dots p-1$,

$$\theta\left(\frac{1}{k!}ad(x)^k(y)\right) = \sum_{j=0}^{k} \frac{(-1)^j}{(k-j)!j!}\theta(x)^{k-j}\theta(y)\theta(x)^j \ .$$

For $k = 1$ this is just the definition of a representation:

$$\theta(ad(x)(y)) = \theta([x,y]) = \theta(x)\theta(y) - \theta(y)\theta(x).$$

Going from k to $k+1$,

$$\begin{aligned}
\theta\left(\frac{1}{(k+1)!}ad(x)^{k+1}(y)\right) &= \frac{1}{k+1}\left(\theta(x)\theta\left(\frac{1}{k!}ad(x)^k(y)\right) - \theta\left(\frac{1}{k!}ad(x)^k(y)\right)\theta(x)\right) \\
&= \sum_{j=0}^{k}\frac{(-1)^j}{k+1}\left(\frac{1}{(k-j)!j!}\theta(x)^{k-j+1}\theta(y)\theta(x)^j\right. \\
&\qquad\qquad \left. - \frac{1}{(k-j)!j!}\theta(x)^{k-j}\theta(y)\theta(x)^{j+1}\right) \\
&= \frac{1}{(k+1)!}\theta(x)^{k+1}\theta(y) \\
&\quad + \sum_{i=1}^{k}\left(\frac{(-1)^i}{(k+1)(k-i)!(i-1)!}\left(\frac{1}{i} + \frac{1}{k+1-i}\right)\right. \\
&\qquad\qquad \left. \cdot\,\theta(x)^{k+1-i}\theta(y)\theta(x)^i\right) \\
&\quad + \frac{(-1)^{k+1}}{(k+1)!}\theta(y)\theta(x)^{k+1} \\
&= \sum_{i=0}^{k+1}\frac{(-1)^i}{(k+1-i)!i!}\theta(x)^{k+1-i}\theta(y)\theta(x)^i \ .
\end{aligned}$$

Finally,

$$\begin{aligned}
\theta(e^{ad(x)}(y)) &= \sum_{k=0}^{p-1}\theta(\frac{1}{k!}ad(x)^k(y)) \\
&= \sum_{i+j=0}^{p-1}\frac{(-1)^j}{i!j!}\theta(x)^i\theta(y)\theta(x)^j \\
&= \sum_{i,j=0}^{p-1}\frac{(-1)^j}{i!j!}\theta(x)^i\theta(y)\theta(x)^j
\end{aligned}$$

$$= \Big(\sum_{i=0}^{p-1} \frac{1}{i!}\theta(x)^i\Big)\theta(y)\sum_{j=0}^{p-1}\frac{(-1)^j}{j!}\theta(x)^j$$
$$= e^{\theta(x)}\theta(y)e^{-\theta(x)},$$

where the third equality holds because (V, θ) is over-restricted: all missing terms are actually zero. $\square$

Proposition 6.1.1.3. *If (V, θ) is a faithful*[142] *over-restricted representation of $\mathfrak{g}$, then the assignment*

$$\phi : e^{\theta(N_p(\mathfrak{g}))} \to G_{\mathfrak{g}}, \quad \phi(e^{\theta(x)}) = e^{ad(x)}, \quad x \in N_p(\mathfrak{g})$$

extends to a surjective homomorphism of abstract groups $\phi : G_V \to G_{\mathfrak{g}}$ whose kernel is central and consists of $\mathfrak{g}$-automorphisms of V.

Proof. Proposition 6.1.1.1 yields the elements $x_1, \ldots, x_n \in N_p(\mathfrak{g})$ for G_V and the elements $x_{n+1}, \ldots, x_m \in N_p(\mathfrak{g})$ for $G_{\mathfrak{g}}$. Combining these elements together, we get surjective algebraic maps with common domain:

$$f : \mathbb{K}^m \to G_V, \quad \widehat{f} : \mathbb{K}^m \to G_{\mathfrak{g}}$$

$$f\Big((a_k)_{k=1}^m\Big) = \prod_{k=1}^{n} e^{\theta(a_k x_k)}, \quad \widehat{f}\Big((a_k)_{k=1}^m\Big) = \prod_{k=n+1}^{m} e^{ad(a_k x_k)} .$$

Let $H = (\mathbb{K}, +)^{*m}$ be the free product of m additive groups. The maps f and $\widehat{f}$ extend to surjective group homomorphisms

$$f^\sharp : H \to G_V, \quad \widehat{f}^\sharp : H \to G_{\mathfrak{g}}$$

so that both G_V and $G_{\mathfrak{g}}$ are quotients of H as abstract groups. Consider an element of the kernel $a_1 * \cdots * a_k \in \ker(f^\sharp)$ where a_i belongs to the $t(i)$-th component of the free product. Clearly,

$$\mathrm{Id}_V = f^\sharp(a_1 * \cdots * a_k) = e^{\theta(a_1 x_{t(1)})}e^{\theta(a_2 x_{t(2)})}\ldots e^{\theta(a_k x_{t(k)})} .$$

Proposition 6.1.1.2 tells us that

$$\theta(e^{ad(a_1 x_{t(1)})}e^{ad(a_2 x_{t(2)})}\ldots e^{ad(a_k x_{t(k)})}(y)) = \theta(y) \ \text{ for all } \ y \in \mathfrak{g}.$$

Since θ is injective it follows that $e^{ad(a_1 x_{t(1)})}\ldots e^{ad(a_k x_{t(k)})} = \mathrm{Id}_{\mathfrak{g}}$, so $a_1 * \cdots * a_k \in \ker(\widehat{f}^\sharp)$. It follows that the homomorphism ϕ is well-defined.

Consider $A := e^{\theta(a_1 x_{t(1)})}\ldots e^{\theta(a_k x_{t(k)})} \in \ker(\phi)$. By Proposition 6.1.1.2,

$$\theta(y) = \theta(\phi(A)(y)) = A\theta(y)A^{-1}$$

[142] A module (V, θ) is called **faithful** if θ is injective.

for all $y \in \mathfrak{g}$. Hence, A commutes with all $\theta(y)$, so $A \in \mathrm{Aut}_{\mathfrak{g}}(V)$. Consequently, A commutes with all $e^{\theta(x)}$, which are generators of G_V. Hence, A is central in G_V. $\square$

It is natural to inquire whether the homomorphism ϕ is a homomorphism of algebraic groups. To prove this, we need a technical result.

Theorem 6.1.1.4. *Suppose that each degree $\mathrm{Deg}_{x_t}(F_j(x_1, \dots x_n))$ of every component of a polynomial map $F = (F_j(x_1, \dots x_n))_{j=1}^m : \mathbb{K}^n \to \mathbb{K}^m$ is less than p. Let Y be the Zariski closure of the image of the polynomial map F. Then the corestricted morphism $\widehat{F} := F|^Y : \mathbb{K}^n \to Y$ is generically smooth.*[143]

The proof is omitted from this thesis, but can be found in the Appendix of [Rumynin and Westaway, 2018]. We can now turn to the main result of this chapter:

Theorem 6.1.1.5. *The following statements hold for a faithful over-restricted finite-dimensional representation (V, θ) of a restricted Lie algebra $\mathfrak{g}$:*

(1) *The map $\phi : G_V \to G_{\mathfrak{g}}$ constructed in Proposition 6.1.1.3 is a homomorphism of algebraic groups.*

(2) *The Lie algebra $\mathrm{Lie}(G_V)$ is isomorphic to $\mathfrak{g}_0$, the Lie subalgebra of $\mathfrak{g}$ generated by all $x \in N_p(\mathfrak{g})$. Therefore, $\mathfrak{g}_0$ is a restricted Lie subalgebra of $\mathfrak{g}$.*[144]

(3) *The derivative $d\eta$ of the natural representation $\eta : G_V \hookrightarrow \mathrm{GL}(V)$ is equal to $\theta|_{\mathfrak{g}_0}$.*

(4) *The derivative $d\phi$ is surjective. Its kernel is $\mathfrak{g}_0 \cap Z(\mathfrak{g})$ where $Z(\mathfrak{g})$ is the centre of $\mathfrak{g}$.*[145]

(5) *The scheme-theoretic kernel $\ker \phi$ is a subgroup scheme of $\mathrm{Aut}_{\mathfrak{g}}(V)$, central in G_V.*

(6) *If $Z(\mathfrak{g}) = 0$, then $\ker \phi$ is discrete.*

Proof. (1) On top of the surjective maps $f : \mathbb{K}^m \to G_V$ and $\widehat{f} : \mathbb{K}^m \to G_{\mathfrak{g}}$, utilised in Proposition 6.1.1.3, using Proposition I.2.2 in [Borel, 1991] once again we can find $x_{m+1}, x_{m+2} \dots, x_k \in N_p(\mathfrak{g})$ such that the image G of the map

$$\widetilde{f} : \mathbb{K}^k \to G_V \times G_{\mathfrak{g}},$$

$$f(a_1, a_2, \dots, a_k) = (e^{\theta(a_1 x_1)} \cdots e^{\theta(a_k x_k)}, e^{ad(a_1 x_1)} \cdots e^{ad(a_k x_k)})$$

[143]Recall that a morphism $\Psi : X \to Y$ of irreducible algebraic varieties over an algebraically closed field is smooth if $d_x\Psi : T_xX \to T_{\Psi(x)}Y$ is surjective for all $x \in X$. The morphism $\Psi : X \to Y$ is called **generically smooth** if there exists a dense open subset $U \subseteq X$ such that $d_x\Psi$ is surjective for all $x \in U$.

[144]A Lie subalgebra $\mathfrak{g}_0$ of a restricted Lie algebra $\mathfrak{g}$ is a **restricted Lie subalgebra** of $\mathfrak{g}$ if $x^{[p]} \in \mathfrak{g}_0$ for all $x \in \mathfrak{g}_0$.

[145]Recall that the **centre** of $\mathfrak{g}$ is $Z(\mathfrak{g}) = \{x \in \mathfrak{g} \,|\, [x, y] = 0 \text{ for all } y \in \mathfrak{g}\}$.

is a closed algebraic subgroup of $G_V \times G_{\mathfrak{g}}$. Extending f and $\widehat{f}$ in the obvious way to the maps f' and $\widehat{f}'$ defined on $\mathbb{K}^k$, we see that $\widetilde{f} = (f', \widehat{f}')$. Hence, G is the graph of the group homomorphism $\phi : G_V \to G_{\mathfrak{g}}$.

Moreover, the first projection $\pi_1 : G \to G_V$ is bijective. Since f' is given by polynomials of degree less than p by construction, Theorem 6.1.1.4 ensures that f' is generically smooth. Since $d\pi_1 \circ d\widetilde{f} = df'$, the differential $d\pi_1$ is surjective at some point. Since π_1 is a morphism of algebraic groups, the differential $d\pi_1$ is surjective at all points. Hence, π_1 is an isomorphism of algebraic groups.[146] Consequently, ϕ is a morphism of algebraic varieties (or groups) since $\phi = \pi_2\pi_1^{-1}$.

(2) Let $\mathfrak{g}_1$ be the linear span of all $x \in N_p(\mathfrak{g})$. Let $(z_1, \ldots, z_k)$ be the standard coordinates on $\mathbb{K}^k$. For all $i = 1, \ldots, k$ the calculation

$$d_0 f'(\frac{\partial}{\partial z_i}) = \frac{d}{dt} e^{\theta(tx_i)}|_{t=0} = \theta(x_i)$$

implies that $\mathrm{Lie}(G_V) \supseteq \mathrm{Im}(d_0 f') = \theta(\mathfrak{g}_1)$. It follows that $\mathrm{Lie}(G_V) \supseteq \theta(\mathfrak{g}_0)$.

By Theorem 6.1.1.4, the differential $d_a f'$ is surjective at some point $a \in \mathbb{K}^k$. If $L_a : G_V \to G_V$ is the left multiplication by $f'(a)^{-1}$, then the Lie algebra $\mathrm{Lie}(G_V)$ is spanned by elements

$$\begin{aligned}
d_{f'(a)} L_a \left(d_a f'(\frac{\partial}{\partial z_i}) \right) &= d_{f'(a)} L_a \left(\frac{d}{dt} e^{\theta(a_1 x_1)} \ldots e^{\theta(a_{i-1} x_{i-1})} e^{\theta((a_i + t) x_i)} e^{\theta(a_{i+1} x_{i+1})} \ldots |_{t=0} \right) \\
&= d_{f'(a)} L_a \left(e^{\theta(a_1 x_1)} \ldots e^{\theta(a_{i-1} x_{i-1})} e^{\theta(a_i x_i)} \theta(x_i) e^{\theta(a_{i+1} x_{i+1})} \ldots \right) \\
&= e^{-\theta(a_n x_n)} \ldots e^{-\theta(a_{i+1} x_{i+1})} \theta(x_i) e^{\theta(a_{i+1} x_{i+1})} \ldots e^{\theta(a_n x_n)} \\
&= \theta \left(e^{-ad(a_n x_n)} \ldots e^{-ad(a_{i+1} x_{i+1})} (x_i) \right) .
\end{aligned}$$

The last equality holds because of Proposition 6.1.1.2. Since all x_j belong to $\mathfrak{g}_0$, the element $e^{-ad(a_n x_n)} \ldots e^{-ad(a_{i+1} x_{i+1})}(x_i)$ also belongs there. Hence, this calculation shows $\mathrm{Lie}(G_V) \subseteq \theta(\mathfrak{g}_0)$. Since θ is faithful, the result follows.

(3) This follows easily from (2).

(4) The same argument as in (1) shows that $d_1\pi_2$ is surjective. Hence, $d_1\phi = d_1\pi_2 \circ d_1\pi_1^{-1}$ is surjective as well.

The second statement follows from the observation that $d_1\phi = ad|_{\mathfrak{g}_0}$. This can be checked on elements $x \in N_p(\mathfrak{g})$ since they generate $\mathfrak{g}_0$ as a Lie algebra:

$$d_1\phi(x) = \frac{d}{dt} e^{ad(tx)}|_{t=0} = ad(x) .$$

(5) This follows from Proposition 6.1.1.3.

(6) This follows from (4) that the differential $d\phi : \mathrm{Lie}(G_V) \to \mathrm{Lie}(G_{\mathfrak{g}})$ is an isomorphism of Lie algebras. Observe that G_V is connected because it is generated as a group by a connected set $e^{\theta(N_p(\mathfrak{g}))}$ containing the identity element. Hence, the kernel of ϕ is discrete. □

[146] See Theorem AG.17.3 in [Borel, 1991] and Theorem 4.6 of Chapter 1 in [Humphreys, 1975].

Let us state an immediate, rather curious corollary of the proof of part (2):

Corollary 6.1.1.6. *Let $\mathfrak{g}$ be a finite-dimensional restricted Lie algebra over an algebraically closed field that admits a faithful over-restricted representation. Let $\mathfrak{g}_1$ be the span of $N_p(\mathfrak{g})$. The following statements, in the notation of the proof of Theorem 6.1.1.5(2), are equivalent:*

(1) *$\mathfrak{g}_1$ is a restricted Lie subalgebra,*

(2) *for some choice of θ and f', the differential $\mathbf{d}_0 f'$ is surjective,*

(3) *for all choices of θ and f', the differential $\mathbf{d}_0 f'$ is surjective.*

Let us contemplate applications of Theorem 6.1.1.5 to integration of representations. Suppose $\mathfrak{g} = \mathrm{Lie}(G)$ where G is a connected algebraic group G (over an algebraically closed field $\mathbb{K}$). The adjoint group G_{ad} is defined as the image of the adjoint representation $\mathrm{Ad} : G \to \mathrm{GL}(\mathfrak{g})$. Notice that G_{ad} is closed because the image of a morphism of algebraic groups is closed.[147] We can compare G_{ad} and $G_{\mathfrak{g}}$ as sets because both are algebraic subgroups of $\mathrm{GL}(\mathfrak{g})$.

Corollary 6.1.1.7. *Suppose that $G_{ad} = G_{\mathfrak{g}}$. The following statements hold for a faithful over-restricted finite-dimensional representation (V, θ) of $\mathfrak{g} = \mathrm{Lie}(G)$:*

(1) *The representation (V, θ) yields a rational representation (V, Θ) of a central extension (that happens to be G_V) of G_{ad} such that $d\Theta(x) = \theta(x)$ for all $x \in \mathfrak{g}_0$.*

(2) *If (V, θ) is a brick,[148] then (V, θ) yields a rational projective representation of G_{ad} such that $d\Theta(\mathbf{x}) = \theta(x)$ for all $x \in \mathfrak{g}_0$.*

Our terminology of pseudo-Chevalley groups is justified by the following example: consider the adjoint representation $\mathfrak{g}$ of a semisimple algebraic group G. Then, barring accidents in small characteristic,[149] $G_{\mathfrak{g}}$ is indeed the adjoint Chevalley group G_{ad}. Notice that the Chevalley group G_{ad} is generated by the exponentials of root vectors $\mathbf{e}_\alpha$. In characteristic zero $ad_{\mathbb{Z}}(\mathbf{e}_\alpha)^4 = 0$, while in positive characteristic $ad(\mathbf{e}_\alpha)^p = 0$ so the exponentials could be different. For instance, if G is of type G_2 in characteristic 3, then the Chevalley exponential $e_{\mathbb{Z}}^{\mathbf{e}_\alpha}$ of the short root vector $\mathbf{e}_\alpha$ contains the divided-power term $ad_{\mathbb{Z}}(\mathbf{e}_\alpha^{(3)})$ but our exponential stops at $ad(\mathbf{e}_\alpha)^2/2$. Similar difficulty appears for all groups in characteristic 2. It is interesting to investigate these questions further: what is the precise relation between $G_{\mathfrak{g}}$ and G_{ad} for simple algebraic groups in characteristic 2 (and the type G_2 group in characteristic 3).

We finish the subsection with an application to semisimple groups. Notice that it is true in characteristic 2 because in this case over-restricted representations are direct sums of the trivial representation.

[147] See [Borel, 1991, I.1.4].
[148] This means that $\mathrm{End}_{\mathfrak{g}} V = \mathbb{K}$.
[149] For instance, taking $p \geqslant 5$.

Corollary 6.1.1.8. *Suppose that G is a connected simply-connected semisimple algebraic group such that $Z(\mathfrak{g}) = 0$. Assume further that if $p = 3$, then G has no components of type G_2. Then a faithful over-restricted finite-dimensional representation (V, θ) of $\mathfrak{g}$ integrates to a rational representation of G.*

6.1.2 Higher Frobenius kernels

In this subsection we take G to be a semisimple simply-connected algebraic group over an algebraically closed field $\mathbb{K}$ of characteristic $p > 0$.[150] We maintain the standard notations for reductive groups used throughout this thesis. In particular, $\mathfrak{g}$ is generated by the elements $\mathbf{e}_\alpha$, where $\alpha \in \Phi$. It is useful to keep in mind that $ad(\mathbf{e}_\alpha)^p = 0$ for all $\alpha \in \Phi$.

Letting G_r be the r-th Frobenius kernel of G, recall that $\mathrm{Dist}(G_r)$ has a divided powers basis

$$\left\{ \prod_{\alpha\in\Phi^+} \mathbf{e}_\alpha^{(m_\alpha)} \prod_{\beta\in\Pi} \binom{\mathbf{h}_\beta}{n_\beta} \prod_{\alpha\in\Phi^+} \mathbf{e}_{-\alpha}^{(m_{-\alpha})} \;\middle|\; 0 \leqslant m_\alpha, n_\beta, m_{-\alpha} < p^r \right\}.$$

Recall further that if $k < p$ then

$$\mathbf{e}^{(k)} = \frac{1}{k!}\mathbf{e}^k \in \mathrm{Dist}(G_1) \ni \binom{\mathbf{h}}{k} = \frac{1}{k!}\mathbf{h}(\mathbf{h}-1)\ldots(\mathbf{h}-k+1)$$

so that $\mathrm{Dist}(G_1)$ is a subalgebra of $\mathrm{Dist}(G_r)$, naturally isomorphic to $U_0(\mathfrak{g})$.[151]

Let us now consider a representation (V, θ) of G_r. As in Subsection 2.3.3, it is naturally a representation of $\mathrm{Dist}(G_r)$ which we also denote by (V, θ). We define exponentials in an analogous way to the previous subsection:

$$Y_\alpha(t) = Y_\alpha^V(t) := e^{\theta(t\mathbf{e}_\alpha)} = \sum_{k=0}^{p^n-1} \theta(t^k \mathbf{e}_\alpha^{(k)}) \in \mathrm{End}(V)$$

$$Z_\alpha(t) = e^{t\mathbf{e}_\alpha} = \sum_{k=0}^{p^n-1} t^k \mathbf{e}_\alpha^{(k)} \in \mathrm{Dist}(G_r)$$

where $t \in \mathbb{K}$ and $\alpha \in \Phi$. Both $Y_\alpha(t)$ and $Z_\alpha(t)$ are invertible. In fact, these are one-parameter subgroups: $Y_\alpha(t)Y_\alpha(s) = Y_\alpha(t+s)$ and $Z_\alpha(t)Z_\alpha(s) = Z_\alpha(t+s)$. Let us generate subgroups by them:

$$G_{r,V} := \langle Y_\alpha(t) \mid \alpha \in \Phi, t \in \mathbb{K} \rangle \leqslant \mathrm{GL}(V),$$

$$\widetilde{G} := \langle Z_\alpha(t) \mid \alpha \in \Phi, t \in \mathbb{K} \rangle \leqslant \mathrm{GL}_1(\mathrm{Dist}(G_r)).$$

Conjugation by G equips $\mathrm{Dist}(G_r)$ with a G-module structure, which we can then re-

[150] We can replace the assumption that $\mathbb{K}$ is algebraically closed with the assumption that G is split up until the Higher Frobenius Conjecture.

[151] See Subsections 2.1.3, 2.3.2 and 2.4.2 for more details.

strict to G_r-module and $\mathrm{Dist}(G_r)$-module structures. The corresponding representation of $\mathrm{Dist}(G_r)$ is precisely the adjoint representation discussed in Subsection 2.2.2, so we denote it by ad. Note that the "usual" adjoint representation on $\mathfrak{g}$ is a subrepresentation under $\mathfrak{g} \hookrightarrow U_0(\mathfrak{g}) \hookrightarrow \mathrm{Dist}(G_r)$ (cf. [Jantzen, 1987, I.7.18, I.7.11(4)]). We also use ad to denote the representation of $\mathrm{Dist}(G)$ on $\mathrm{Dist}(G_r)$; this restricts to the above ad on $\mathrm{Dist}(G_r)$.

We say that (V,θ) is r-**over-restricted** if $\theta(\mathbf{e}_\alpha^{(k)}) = 0$ for all $k \geqslant \lfloor (p^r+1)/2 \rfloor$, and all $\alpha \in \Phi$. Notice that if $p^r = 2$ then this condition forces (V,θ) to be a direct sum of the copies of the trivial module.

Proposition 6.1.2.1. *(cf. Proposition 6.1.1.2) If (V,θ) is an r-over-restricted representation of* $\mathrm{Dist}(G_r)$*, then*

$$\theta\Big(ad(Z_\alpha(t))(d)\Big) = Y_\alpha(t)\theta(d)Y_\alpha(-t)$$

for all $t \in \mathbb{K}$, $\alpha \in \Phi$ and $d \in \mathrm{Dist}(G_r)$.

Proof. We write ad using Sweedler's Σ-notation:[152]

$$ad(x)(d) = \sum_{(x)} x_{(1)} d S(x_{(2)}) \quad \text{for all } x, d \in \mathrm{Dist}(G_r).$$

Since $\Delta(\mathbf{e}_\alpha^{(k)}) = \sum_{i+j=k} \mathbf{e}_\alpha^{(i)} \otimes \mathbf{e}_\alpha^{(j)}$ and $S(\mathbf{e}_\alpha^{(k)}) = (-1)^k \mathbf{e}_\alpha^{(k)}$, we get

$$\theta(ad(t^k\mathbf{e}_\alpha^{(k)})(d)) = \theta\left(\sum_{i+j=k} (-1)^j t^k \mathbf{e}_\alpha^{(i)} d \mathbf{e}_\alpha^{(j)}\right) = \sum_{i+j=k} \theta(t^i\mathbf{e}_\alpha^{(i)})\theta(d)\theta((-t)^j\mathbf{e}_\alpha^{(j)}).$$

Hence,

$$\theta\Big(ad(Z_\alpha(t))(d)\Big) = \sum_{k=0}^{p^r-1} \sum_{i+j=k} \theta(t^i\mathbf{e}_\alpha^{(i)})\theta(d)\theta((-t)^j\mathbf{e}_\alpha^{(j)}).$$

On the other hand, we have

$$Y_\alpha(t)\theta(d)Y_\alpha(-t) = \sum_{i,j=0}^{p^r-1} \theta(t^i\mathbf{e}_\alpha^{(i)})\theta(d)\theta((-t)^j\mathbf{e}_\alpha^{(j)}).$$

The result follows from the fact that V is r-over-restricted. □

It is useful to remind the reader that $\mathfrak{g}$ can be recovered inside $\mathrm{Dist}(G_r)$ as the set of primitive elements:

$$\mathfrak{g} = P(\mathrm{Dist}(G_r)) = \{d \in \mathrm{Dist}(G_r) \mid \Delta(d) = d \otimes 1 + 1 \otimes d\}.$$

This explains why $\mathfrak{g}$ is a submodule of $\mathrm{Dist}(G_r)$ under the adjoint action: we leave it to the reader to check that $ad(x)(d) \in P(\mathrm{Dist}(G_r))$ for all $x \in \mathrm{Dist}(G_r)$ and

[152]See I.7.18 in [Jantzen, 1987]

$d \in P(\mathrm{Dist}(G_r))$.

Proposition 6.1.2.2. *Let (V,θ) be an r-over-restricted representation of* $\mathrm{Dist}(G_r)$*, faithful on $\mathfrak{g}$. Then the assignment*

$$\phi(Y_\alpha^V(t)) = Y_\alpha^{\mathfrak{g}}(t) \ (= e^{ad(t\mathbf{e}_\alpha)})$$

extends to a surjective homomorphism of groups $\phi : G_{r,V} \to G_{r,\mathfrak{g}}$, whose kernel consists of $\mathfrak{g}$-automorphisms of V.

Proof. The fact that ϕ is a well-defined homomorphism is proved in a similar way as in Proposition 6.1.1.3. Let $H = *_\alpha U_\alpha$ be the free product of (additive) root subgroups. Both $G_{r,V}$ and $G_{r,\mathfrak{g}}$ are naturally quotients of H. If $W_{\beta_1}(t_1) * \cdots * W_{\beta_m}(t_m) \in \ker(H \to G_{r,V})$ then

$$Y_{\beta_1}^V(t_1) \ldots Y_{\beta_m}^V(t_m) = I_V \ .$$

Proposition 6.1.2.1 tells us that for all $d \in \mathfrak{g}$

$$\theta(ad(Z_{\beta_1}(t_1))ad(Z_{\beta_2}(t_2)) \ldots ad(Z_{\beta_m}(t_m))(d)) = \theta(Y_{\beta_1}^{\mathfrak{g}}(t_1) \ldots Y_{\beta_m}^{\mathfrak{g}}(t_m)(d)) = \theta(d).$$

Since θ is faithful on $\mathfrak{g}$, $Y_{\beta_1}^{\mathfrak{g}}(t_1)Y_{\beta_2}^{\mathfrak{g}}(t_2) \ldots Y_{\beta_m}^{\mathfrak{g}}(t_m) = I_{\mathfrak{g}}$, hence $W_{\beta_1}(t_1)*\cdots*W_{\beta_m}(t_m) \in \ker(H \to G_{n,\mathfrak{g}})$. Thus, the homomorphism ϕ is well-defined.

Suppose $A = Y_{\beta_1}^V(t_1) \ldots Y_{\beta_m}^V(t_m) \in \ker(\phi)$. By above, $\theta(d) = \theta(\phi(A)(d)) = A\theta(d)A^{-1}$ for all $d \in \mathfrak{g}$. Hence, $A \in \mathrm{Aut}_{\mathfrak{g}}(V)$. □

If the adjoint representation is r-over-restricted, we can identify the adjoint group G_{ad} with $G_{r,\mathfrak{g}}$. Proposition 6.1.2.2 yields an exact sequence of abstract groups

$$1 \to Z_{(r),V} \to G_{r,V} \xrightarrow{\phi} G_{ad} \to 1$$

where $Z_{r,V}$ is the kernel of ϕ. To tie up loose ends we need to address the algebraic group properties of this sequence:

Higher Frobenius Conjecture. *Suppose that G is a semisimple connected algebraic group over an algebraically closed field $\mathbb{K}$ of characteristic $p > 0$. The following statements should hold for an r-over-restricted finite-dimensional representation (V,θ) of G_r, faithful on $\mathfrak{g}$:*

(1) *The map $\phi : G_{r,V} \to G_{r,\mathfrak{g}}$ constructed in Proposition 6.1.2.2 is a homomorphism of algebraic groups.*

(2) *If $(\mathfrak{g}, ad)$ is r-over-restricted then $\phi : G_{r,V} \to G_{r,\mathfrak{g}}$ is a central extension of algebraic groups.*

(3) *If $(\mathfrak{g}, ad)$ is r-over-restricted then (V,θ) extends to a rational representation of the simply-connected group G_{sc}.*

6.2 Applications

6.2.1 Applications of Higher Frobenius Conjecture

Once again, G is a semisimple simply-connected algebraic group over an algebraically closed field $\mathbb{K}$ of characteristic $p > 0$. Let (P, θ) be a projective indecomposable $U_0(\mathfrak{g})$-module. The Humphreys-Verma Conjecture states that (P, θ) extends to a G-module. A similar statement for higher Frobenius kernels follows from the Humphreys-Verma Conjecture.[153] Let us examine what our new Higher Frobenius Conjecture can contribute towards this long-standing conjecture.

Let T be the maximal torus of G. TG_r-modules are the same as $X(T)$-graded G_r-modules. We can control the condition of being r-over-restricted for them by monitoring their weights

$$X(V) := \{\lambda \in X(T) \mid V_\lambda \neq 0\}.$$

We define **the height of** V by the following formula:

$$\xi(V) := \inf\{n \in \mathbb{N} \mid \forall \alpha \in \Phi \quad X(V) \cap (X(V) + n\alpha) = \varnothing\}.$$

Clearly $\theta(\mathbf{e}_\alpha^{(\xi(V))}) = 0$ is guaranteed for a TG_r-module (V, θ). Hence, the next proposition immediately follows from the Higher Frobenius Conjecture:

Proposition 6.2.1.1. *Suppose that the Higher Frobenius Conjecture holds for a connected simply-connected semisimple algebraic group G such that $Z(\mathfrak{g}) = 0$. Assume further that if $p^r = 3$, then G has no components of type G_2. Let (V, θ) be a TG_r-module, faithful as a $\mathfrak{g}$-module, such that $p^r \geqslant 2\xi(V) - 1$ if p is odd, or $p^r \geqslant 2\xi(V)$ if $p = 2$. Then (V, θ) can be extended to a G-module.*

It follows that if a TG_1-module can be extended to a TG_r-module for sufficiently large r, then it can be extended to a G-module. Due to particular significance of projective $U_0(\mathfrak{g})$-modules we state this observation for them as a proposition. Recall that $\rho = \frac{1}{2}\sum_{\alpha\in\Phi^+}\alpha$ is the half-sum of positive roots. Let $a = \max_{1\leqslant i\leqslant n}(a_i)$ where $2\rho = \sum_{\alpha_i\in\Pi} a_i\alpha_i$ for $a_i \in \mathbb{Z}$.

Proposition 6.2.1.2. *Suppose that the Higher Frobenius Conjecture holds for a connected simply-connected semisimple algebraic group G such that $Z(\mathfrak{g}) = 0$. Let P be a projective indecomposable $U_0(\mathfrak{g})$-module. Suppose P extends to a rational G_r-module where*

$$r \geqslant \log_p(4a(p-1)+1).$$

if p is odd, or

$$r \geqslant \log_2(a+1) + 2$$

if $p = 2$. Then P extends to a G-module.

[153]See Remark II.11.18 in [Jantzen, 1987].

Table 6.1: Coxeter numbers and coefficients a (Classical type)

	A_{2l+1}	A_{2l}	B_n	C_n	D_n
$2h-2$	$4l+2$	$4l$	$4n-2$	$4n-2$	$4n-6$
a	$(l+1)^2$	$l(l+1)$	n^2	$(n-1)(n+2)$	$(n+1)(n-2)$

Table 6.2: Coxeter numbers and coefficients a (Exceptional type)

	E_6	E_7	E_8	F_4	G_2
$2h-2$	22	34	58	22	10
a	42	96	270	42	10

Proof. It is known that P is a TG_1-module.[154] Clearly, $\xi(P) \leqslant \xi(U_0(\mathfrak{g}))$. From the Poincaré-Birkhoff-Witt basis, it follows that the "top" grade of the grading on $U_0(\mathfrak{g})$ is attained by the element $\prod_{\alpha\in\Phi^+} \mathbf{e}_\alpha^{p-1}$. This has grade $2(p-1)\rho$. Similarly, the "bottom" grade is $-2(p-1)\rho$. Thus, $\xi(U_0(\mathfrak{g})) \leqslant 2(p-1)a+1$ and the condition in Proposition 6.2.1.1, when p is odd, becomes $p^r \geqslant 2\xi(U_0(\mathfrak{g}))-1$; for this to be true, it is enough that $p^r \geqslant 4a(p-1)+1$. When $p=2$, the condition becomes $2^{r-1} \geqslant \xi(U_0(\mathfrak{g}))$, for which it is enough that $2^{r-1} \geqslant 2a+1$ or equivalently $2^{r-2} \geqslant a+1$. $\square$

For the reader's benefit we add four tables. The first two contain the values of $2h-2$ and a. The third and fourth list the smallest prime p_0 for all groups up to rank 8 so that extension of P to a rational G_r-module guarantees an extension to a rational G-module as soon as $p \geqslant p_0$ (the column is the type of G, the row is G_r). They also list the smallest r such that extension to G_r ensures extension to G for $p=2,3,5$. For Table 6.3, we omit this list for $p=3,5$ since in these cases the requirement becomes vacuous – no extension to a higher Frobenius kernel is needed. Some of the entries are marked with the dagger †. This signifies the presence of a non-trivial centre $Z(\mathfrak{g}) \neq 0$.

6.2.2 Examples

The heights can be computed for Weyl modules.[155] Let $V(\lambda)$ be the Weyl module with the highest weight $\lambda = \sum_i k_i\varpi_i$ written in the basis of fundamental weights. It

[154] See II.11.3 in [Jantzen, 1987].

[155] The Weyl module $V(\lambda)$, for $\lambda \in X(T)$, is defined as the contravariant dual of the G-module $\nabla(\lambda)$, where $\nabla(\lambda)$ is as in Subsection 2.4.4.

Table 6.3: G_r-extension requirements in characteristic p (Smaller ranks)

	G_2	G_3	G_4	G_5	2
A_1	3	$^\dagger 2$	$^\dagger 2$	$^\dagger 2$	$^\dagger G_3$
A_2	7	$^\dagger 3$	2	2	G_4
B_2	17	5	3	$^\dagger 2$	$^\dagger G_5$
G_2	41	7	3	3	G_6
A_3	17	5	3	$^\dagger 2$	$^\dagger G_5$
B_3	37	7	3	3	$^\dagger G_6$
C_3	41	7	3	3	$^\dagger G_6$
A_4	23	$^\dagger 5$	3	2	G_5
B_4	67	11	5	3	$^\dagger G_7$
C_4	71	11	5	3	$^\dagger G_7$
D_4	41	7	3	3	G_6
A_5	37	7	$^\dagger 3$	$^\dagger 3$	G_6
B_5	101	11	5	3	$^\dagger G_7$
C_5	113	11	5	3	$^\dagger G_7$
D_5	71	11	5	3	G_7

Table 6.4: G_r-extension requirements in characteristic p (Larger ranks)

	G_2	G_3	G_4	G_5	2	3	5
F_4	167	13	7	5	G_8	G_6	G_5
A_6	47	$^\dagger 7$	5	3	G_6	G_5	G_4
B_6	149	13	5	5	$^\dagger G_8$	G_6	G_4
C_6	161	13	7	5	$^\dagger G_8$	G_6	G_5
D_6	113	11	5	3	G_7	G_5	G_4
E_6	167	13	7	5	G_8	$^\dagger G_6$	G_5
A_7	67	11	5	3	$^\dagger G_7$	G_5	G_4
B_7	193	17	7	5	$^\dagger G_8$	G_6	G_5
C_7	221	17	7	5	$^\dagger G_8$	G_6	G_5
D_7	161	13	7	5	G_8	G_6	G_5
E_7	383	23	7	5	$^\dagger G_9$	G_7	G_5
A_8	79	11	5	3	G_7	$^\dagger G_5$	G_4
B_8	257	17	7	5	$^\dagger G_9$	G_6	G_5
C_8	281	17	7	5	$^\dagger G_9$	G_6	G_5
D_8	221	17	7	5	G_8	G_6	G_5
E_8	1087	37	11	7	G_{11}	G_7	G_6

follows from the description of $V(\lambda)$ by generators and relations[156] that

$$\xi(V(\lambda)) \leqslant 1 + 2\max_i \frac{(\lambda, \alpha_i)}{(\alpha_i, \alpha_i)} = 1 + \max_i k_i \ .$$

This means that the Weyl modules with $k_i \leqslant (p-1)/2$ for all $i = 1, \ldots, r$ are over-restricted. For instance, if $\mathfrak{g}$ is of type A_2 then (for $p > 3$) the Weyl module $V(\frac{p-1}{2}\omega_1 + \frac{p-1}{2}\omega_2)$ is the only over-restricted Weyl module outside the first closed p-alcove (under the $\bullet$-action): indeed, $k_1 + k_2 = p - 1 > p - 2$. Thus, most (but not all) over-restricted modules are semisimple in this case.

On the other hand, if $\mathfrak{g}$ is of type G_2 and α_1 is short, then the over-restricted Weyl module $V(\frac{p-1}{2}\omega_1 + \frac{p-1}{2}\omega_2)$ lies inside the ninth p-alcove (if $p > 3$):

$$k_1 + 2k_2 = \frac{3}{2}(p-1) < 2p - 3, \ k_1 + 3k_2 = 2(p-1) > 2p - 4, \ k_1 = \frac{p-1}{2} < p - 1.$$

Ninth in this context means that there are eight dominant p-alcoves below it. Thus, in type G_2 there are many over-restricted non-semisimple modules.

6.2.3 Conclusion

What have we achieved in this chapter and Chapter 5? Suppose G is a semisimple algebraic group with Lie algebra $\mathfrak{g}$. Which concrete $\mathfrak{g}$-modules can we now extend to G-modules? One evident case is when (V, θ) is an indecomposable G-stable $\mathfrak{g}$-module such that G acts trivially on $\mathrm{Aut}_{\mathfrak{g}}(V, \theta)$. By combination of Corollary 5.2.2.6, Lemma 5.2.2.8 and the cohomology vanishing of the trivial module,[157] $H^2_{Rat}(G, G_1; A) = 0 = H^1_{Rat}(G, G_1; A)$ for all A, constituents of $\mathrm{Aut}_{\mathfrak{g}}(V, \theta)$. Thus, the $\mathfrak{g}$-module structure of such (V, θ) extends uniquely to a G-module structure.

It is possible to ensure the triviality of the action if one can control the weights. The weights of simple constituents of $\mathrm{Aut}_{\mathfrak{g}}(V, \theta)$ must be divisible by p because G_1 acts trivially. On the other hand, the weights of $V \otimes V^*$ are the differences of weights of V. Thus, the difference of any two distinct weights of V must be divisible by p, and this can be made impossible by bounding $\xi(V)$. We therefore have a version of Proposition 6.2.1.1:

Proposition 6.2.3.1. *Let (V, θ) be a G-stable TG_1-module such that $p \geqslant 2\xi(V) - 1$. Then (V, θ) can be uniquely extended to a G-module.*

[156] See Theorem 21.4 in [Humphreys, 1972].
[157] See II.4.11 in [Jantzen, 1987].

Bibliography

[Ballard, 1978] J. Ballard, *Injective modules for restricted enveloping algebras*, Math. Z. **193**(1) (1978), 57–63.

[Bendel et al., 2019] C. Bendel, D. Nakano, C. Pillen, P. Sobaje, *Counterexamples to the tilting and (p, r)-filtration conjectures*, arXiv:1901.06687, (2019).

[Berthelot, 1996] P. Berthelot, *$\mathcal{D}$-modules arithmétiques. I. Opérateurs différentiels de niveau fini*, Ann. Sci, Éc. Norm. Supér. **29**(4) (1996), 185–272.

[Bezrukavnikov et al., 2008] R. Bezrukavnikov, I. Mirković, D. Rumynin, *Localization of modules for a semisimple Lie algebra in prime characteristic*, Ann. of Math. **167**(2) (2008), 945–991.

[Borel, 1991] A. Borel, *Linear Algebraic Groups. Second edition*, Graduate Texts in Mathematics, Springer-Verlag, New York, 1991.

[Bourbaki, 1975] N. Bourbaki, *Groupes et algèbres de Lie*, Hermann, Paris 1971 (ch. I), 1972 (ch. II/III), 1968 (ch. IV–VI), 1975 (ch. VII/VIII).

[Brown and Goodearl, 1997] K. Brown, K. Goodearl, *Homological aspects of Noetherian PI Hopf algebras or irreducible modules and maximum dimension*, J. Algebra **198**(1) (1997), 240–265.

[Brown and Goodearl, 2002] K. Brown, K. Goodearl, *Lectures on Algebraic Quantum Groups*, Advanced Courses in Mathematics, CRM Barcelona, Birkäuser Verlag, Basel, 2002.

[Brown and Gordon, 2001] K. Brown, I. Gordon, *The ramification of centres: Lie algebras in positive characteristic and quantised enveloping algebras*, Math. Z. **238**(4) (2001), 733–779.

[Cline, Parshall and Scott, 1980] E. Cline, B. Parshall, L. Scott, *On the tensor product theorem for algebraic groups*, J. Algebra **63**(1) (1980), 264–267.

[Curtis, 1960] C. Curtis, *Representations of Lie algebras of classical type with applications to linear groups*, J. Math. Mech., **9** (1960), 307–326.

[Dade, 1981] E. Dade, *Extending irreducible modules*, J. Algebra **72**(2) (1981), 374–403.

[Demazure and Gabriel, 1970] M. Demazure, P. Gabriel, *Groupes algébriques, Tome 1: Géométrie algébrique, généralités, groupes commutatifs*, Masson & Cie, Éditeur, Paris; North Holland Publishing Co., Amsterdam, 1970.

[Dieudonné and Grothendieck, 1960–67] J. Dieudonné, A. Grothendieck, *Éléments de Géométrie Algébrique*, Publ. Math. Inst. Hautes Études Sci. **4, 8, 11, 17, 20, 24, 28, 32**, (1960–67).

[Donkin, 1982] S. Donkin, *Note on the characters of the projective modules for the infinitesimal subgroups of a semisimple group*, Math. Scand. **51**(1) (1982), 142–150.

[Drozd and Kirichenko, 1994] Y Drozd, Y. Kirichenko, *Finite Dimensional Algebras (Translated)*, Springer-Verlag, Berlin, 1994.

[Friedlander and Parshall, 1988] E. Friedlander, B. Parshall, *Modular representation theory of Lie algebras*, Amer. J. Math. **110**(6) (1988), 1055–1093.

[Friedlander and Parshall, 1990] E. Friedlander, B. Parshall, *Deformations of Lie algebra representations*, Amer. J. Math. **112**(3) (1990), 375–395.

[Hall, 2015] B. Hall, *Lie groups, Lie algebras, and representations. An elementary introduction. Second edition*, Graduate Texts in Mathematics, 222, Springer, Cham., 2015.

[Hashimoto et al., 2006] Y. Hashimoto, M. Kaneda, D. Rumynin, *On localization of $\overline{D}$-modules*, Representations of algebraic groups, quantum groups and Lie algebras, Contemp. Math. **413** (2006), 43–62.

[Hogeweij, 1982] G. Hogeweij, *Almost-classical Lie algebras. I*, Indag. Math., **44** (1982), 441–452.

[Humphreys, 1972] J. Humphreys, *Introduction to Lie algebras and representation theory*, Graduate Texts in Mathematics, Vol. 9, Springer-Verlag, New York-Berlin, 1972.

[Humphreys, 1975] J. Humphreys, *Linear Algebraic Groups*, Graduate Texts in Mathematics, No. 21, Springer-Verlag, New York-Heidelberg, 1975.

[Humphreys, 1976] J. Humphreys, *Ordinary and Modular representations of Chevalley groups*, Lecture Notes in Mathematics, Vol. 528, Springer-Verlag, Berlin-New York, 1976.

[Humphreys and Verma, 1973] J. Humphreys, D. Verma, *Projective modules for finite Chevalley groups*, Bull. Amer. Math. Soc. **79** (1973), 467-–469.

[Jacobson, 1952] N. Jacobson, *A note on Lie algebras of characteristic p*, Amer. J. Math. **79**, (1952), 357–359.

[Jacobson, 1989] N. Jacobson, *Basic Algebra. II. Second Edition*, W.H. Freeman and Company, New York, 1989.

[Jantzen, 1980] J. Jantzen, *Darstellungen halbeinfacher Gruppen und ihrer Frobenius-Kerne*, J. Reine. Angew. Math. **317** (1980), 157–199.

[Jantzen, 1987] J. Jantzen, *Representations of algebraic groups*, Pure and Applied Mathematics, vol. 131, Academic Press, 1987.

[Jantzen, 1997] J. Jantzen, *Representations of Lie algebras in prime characteristic*, in Proc. NATO ASI Representation Theory and Algebraic Geometry, Montreal (1997), 185–235 (A. Broer, ed.) Kluwer, Dordrecht (1998).

[Jantzen, 2004] J. Jantzen, *Representations of Lie algebras in positive characteristic*, in Representation Theory of Algebraic Groups and Quantum Groups, Adv. Stud. Pure Math. **40** (2004), 175–218, Math. Soc. Japan, Tokyo.

[Kac and Weisfeiler, 1971] V. Kac, B. Weisfeiler, *The irreducible representations of Lie p-algebras*, Funktsional. Anal. i Prilozhen. **5**(2), (1971), 28–36.

[Kac and Weisfeiler, 1976] V. Kac, B. Weisfeiler, *Coadjoint action of a semisimple algebraic group and the centre of the universal enveloping algebra in characteristic p*, Indag. Math. (N.S,) **38**(2), (1976), 136–151.

[Kaneda and Ye, 2007] M. Kaneda, J. Ye, *Equivariant localization of $\overline{D}$-modules on the flag variety of the symplectic group of degree 4*, J. Algebra **309**(1), (2007), 236–281.

[Karpilovsky, 1989] G. Karpilovsky, *Clifford theory for group representations*, Mathematical Studies 156, North Holland, Netherlands, 1989.

[Kostant, 1966] B. Kostant, *Groups over Z*, Proc. Sympos. Pure Math. **9** (1966), 90–98.

[McConnell and Robson, 2001] J. McConnell, J. Robson, *Noncommutative Noetherian rings. Revised edition,* Graduate Studies in Mathematics, 30. American Mathematical Society, Providence, RI, 2001.

[Milne, 2017] J. Milne, *Algebraic groups. The theory of group schemes of finite type over a field*, Cambridge Studies in Advanced Mathematics, 170, Cambridge University Press, Cambridge, 2017.

[Montgomery, 1993] S. Montgomery, *Hopf algebras and their actions on rings*, CBMS Regional Conference Series in Mathematics, Vol. 82, Amer. Math. Soc., Providence, 1993.

[Premet, 1995] A. Premet, *Irreducible representations of Lie algebras of reductive groups and the Kac-Weisfeiler conjecture*, Invent. Math. **121**(1), (1995), 79–117.

[Premet and Skryabin, 1999] A Premet, S. Skryabin, *Representations of restricted Lie algebras and families of associative $\mathcal{L}$-algebras*, J. Reine Angew. Math. **507**, (1999), 189–218.

[Rosenlicht, 1956] M. Rosenlicht, *Some basic theorems on algebraic groups*, Amer. J. Math **78** (1956), 401–443.

[Rowen, 1980] L. Rowen, *Polynomial Identities in Ring Theory*, Pure and Applied Mathematics 84, Academic Press Inc. [Harcourt Brace Jovanovich, Publishers], New York-London, 1980.

[Rowen, 1991] L. Rowen, *Ring Theory. Student Edition*, Academic Press Inc., Boston, MA, 1991.

[Rumynin and Westaway, 2018] D. Rumynin, M. Westaway, *Integration of Modules I: Exponentials*, arXiv:1807.08698, (2018).

[Rumynin and Westaway, 2019] D. Rumynin, M. Westaway, *Integration of Modules I: Stability*, Pacific J. Math. **301**(2), (2019), 575–600.

[Schneider, 1990] H. Schneider, *Representation theory of Hopf-Galois extensions*, Israel J. Math **72**(1–2) (1990), 196–231.

[Schneider, 1993] H. Schneider, *Some remarks on exact sequences of quantum groups*, Comm. Algebra **21**(9) (1993), 3337–3357.

[Schneider, 1994] H. Schneider, *Hopf-Galois extensions, crossed products, and Clifford Theory*, in "Advances in Hopf Algebras," Lecture Notes in Pure and Applied Mathematics, Vol 158, Dekker, New York, 1994.

[Sobaje, 2017] P. Sobaje, *On liftings of projective indecomposable $G_{(1)}$-modules*, J. Algebra **475** (2017), 61–79.

[Steinberg, 1968] R. Steinberg, *Lectures on Chevalley groups*, Notes prepared by John Faulkner and Robert Wilson, Yale University, New Haven, Conn., 1968.

[Steinberg, 1963] R. Steinberg, *Representations of algebraic groups*, Nagoya Math. J. **22** (1963), 33–56.

[Sweedler, 1967] M. Sweedler, *Hopf algebras with one grouplike element*, Trans. Amer. Math. Soc. **127** (1967), 515–526.

[Thévenaz, 1983] J. Thévenaz, *Extensions of group representations from a normal subgroup*, Communications in Algebra **11**(4) (1983), 391–425.

[van der Kallen, 1973] W. van der Kallen, *Infinitesimally central extensions of Chevalley groups*, Lecture Notes in Math. 356, Springer, Berlin, 1973.

[Weil, 1955] A. Weil, *On algebraic groups of transformations*, Amer. J. Math. **77** (1955), 355–391.

[Westaway, 2018] M. Westaway, *Higher deformations of Lie algebra representations I*, arXiv:1807.00660, (2018). To appear.

[Westaway, 2019] M. Westaway, *Higher deformations of Lie algebra representations II*, arXiv:1904.10860, (2019). To appear.

[Witherspoon, 1999] S. Witherspoon, *Clifford correspondence for finite-dimensional Hopf algebras*, J. Algebra **218**(2) (1999), 608–620.

[Xanthopoulos, 1992] S. Xanthopoulos, *On a question of Verma about decomposable representations of algebraic groups and their Lie algebras*, PhD Thesis, Queen Mary University of London, 1992.