UNIPOTENT ALGEBRAIC GROUPS

A dissertation

submitted by

Seth J. Rothschild

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

in

Mathematics

TUFTS UNIVERSITY

May 2017

Adviser: Professor George J. McNinch

Abstract

Let $\mathbf{G}_a$ be the additive algebraic group over an algebraically closed field k of odd characteristic. This thesis considers group extensions $\mathbf{H}$ of $\mathbf{G}_a$ by $\mathbf{G}_a$. By [Ros56], every unipotent group has a closed subgroup isomorphic to $\mathbf{G}_a$ and a quotient which is isomorphic to $\mathbf{G}_a$. By studying extensions of $\mathbf{G}_a$ by $\mathbf{G}_a$, we study every connected two dimensional unipotent group.

In Chapter 4, we provide the description of an arbitrary $\mathbf{H}$ with cohomological data as in [Jan03] and the description of Lazard's exponential as in [BD06]. From the orbit method, we give the representations of the finite group $H = \mathbf{H}(\mathbf{F}_q)$ in terms of the cohomological data of the extension $\mathbf{H}$.

In Chapter 5 we find conditions for an algebraic torus $T = \mathbf{G}_m(\mathbf{F}_q)$ to act on H by automorphisms. Given $G = H \rtimes T$, we provide a description of the representations of G both over a characteristic 0 field and over a field of characteristic ℓ which divides the order of T using the representations found in 4.

Other "terminal" results appear where appropriate. We show that every perfect group scheme is a subgroup of a product of perfectized Witt vectors in Chapter 3 by modifying an argument of Serre in [Ser88] and give a bound on the dimension of the cohomology of an arbitrary reductive group from first principles in 6. Matrix embeddings for arbitrary two dimensional $\mathbf{H}$ can be found in Chapter 4.

To Mom, Dad, Ethan

and Hayley, who tolerate

all my absurd plans.

Acknowledgments

This thesis would not have been possible without help and support from many individuals. Primary among those is my advisor, George McNinch, to whom I owe the vast majority of my mathematical intuition and biases. During my time here at Tufts he has communicated to me both the topic of this thesis and the ideas behind many of the proofs found here. I am greatly indebted to him for his positive influence on my work and for his enduring patience.

I would like to thank my committee, Paul Sobaje, Robert Lemke-Oliver and Richard Weiss for taking the time to read and comment on this manuscript. Their contributions, including but not limited to helping me squash bugs, improved this thesis substantially and as a byproduct improved me as a writer. I would also like to thank Nate Fisher and Chris O'Donnell for many helpful comments on this thesis.

The mathematics graduate community here at Tufts plays a larger-than-average role in supporting our own existence. We have a communal structure that helped me pass my qualifying classes, learn how to teach, and prepare my candidacy exam very quickly. They even tolerated (and occasionally encouraged) my student seminar talks. There are too many graduate students current and former to thank here by name, however, I will note that Burns Healy, Garret Laforge, Chris O'Donnell and Andrew Sánchez contributed to literally everything in this paragraph and more.

Lastly, I would like to thank Ethan, Kenneth, Ryan, Alex and Chris P. whose friendship has been invaluable and my family for their unequivocal support.

Contents

Chapter 1

Introduction

There was, at some point, hope of creating a thesis that was readable by the public. The moral imperative is to convey mathematics as readably as possible so that it can reach the largest possible audience. Not only that, but it would be really nice to talk to friends and family about what I've been doing for the last five years.

As mathematicians, we're pretty used to not being able to explain what we do to non-mathematicians. David Mumford has a sequence of fascinating blog posts at [Mum14] about trying to write an obituary for Grothendieck in *Science*. He writes

> "The gap between the world I have lived in and that even of scientists has never seemed larger. I am prepared for lawyers and business people to say they hated math and not to remember any math beyond arithmetic, but this!?"

To do a thesis in a straightforward way is a goal I believe in, but one that I would have been entirely unable to achieve. In writing my research, it quickly became apparent that there were at least two major obstructions to writing for the "lawyers and business people" who generate my immediate family.

First, there is an enormous literature needed to *define* Algebraic Groups, the fundamental object of study of this thesis. Definitions, examples, and theorems are pulled from a wide range of textbooks. Primarily, I used [DF04] and [Lan84] for Algebra, [AM69] for commutative algebra, [Mum88] for varieties and schemes, and [Spr98] for algebraic groups. For the required representation theory, I used [Ser77] and [CR06] and for category theory and homological algebra I used [Jan03] and [Wei94]. Background chapters from those books are, quite selfishly, excluded as much as possible.

The second obstruction is in writing style. While I'm confident in my ability to entertain you for most of the introduction, I don't have many funny things to say when introducing k-group functors. Moreover, if I were capable of writing something that was both one hundred pages and entertaining, I probably wouldn't write it on this.

The target audience for this thesis is a graduate student with a good working knowledge of graduate algebra. For those readers, the remainder will likely be challenging but possible. Interested professors should skim Chapter 2 and begin reading in Chapter 3. If you, like most people, are not in one of those two categories, there is a real chance it is not worth your time to read beyond the introduction.

This thesis deals with the *structure and representations of unipotent algebraic groups*. There are two building blocks for a linear algebraic group: reductive groups and unipotent groups. Many theorems which are true of reductive groups are not true of those which are unipotent. As an example, reductive algebraic groups over a sufficiently nice (algebraically closed) field have a complete classification. Not only does a classification not exist for unipotent groups, it is not expected that one ever will.

It is now necessary to be temporarily technical, but the non-mathematical portions of the introduction will resume in a few paragraphs. For any algebraic group G defined over $\mathbf{F}_q$, the finite points $G(\mathbf{F}_q)$ are also a group. Those groups have representations, group homomorphisms $G(\mathbf{F}_q) \to \mathrm{GL}_n(\mathbf{C})$, even though G doesn't itself have an interesting theory of complex representations.

The situation was improved by Lusztig with the concept of a "character sheaf" for reductive groups in a series of papers starting with [Lus85]. Character sheaves are a construction of a geometric theory of characters which is as close as possible to the character theory of the underlying finite points $G(\mathbf{F}_q)$. Naturally, it took time to modify definitions which worked for reductive groups into definitions that would be useful for groups which are unipotent. The thesis work of Boyarchenko [Boy07] and subsequent papers with Drinfeld ([Boy13], [Boy10], [BD14]) do exactly that.

Fundamental to that study is the notion of $\mathbb{L}$-packets, the fibers of a map

$$\mathrm{Irr}(G(\mathbf{F}_q), \mathbf{C}^\times) \to \mathrm{Irr}(G, \mathbf{C}^\times)^{\mathrm{Gal}(k/\mathbf{F}_q)}$$

where k is an algebraic closure of $\mathbf{F}_q$. Two irreducible representations of $G(\mathbf{F}_q)$ are $\mathbb{L}$-indistinguishable if they have the same image in $\mathrm{Irr}(G, \mathbf{C}^\times)$. The smallest possible example of groups with nontrivial $\mathbb{L}$-packets was introduced in [BD06], the "fake-Heisenberg" groups.

This thesis generalizes those groups and finds all two dimensional unipotent groups with nontrivial $\mathbb{L}$-packets explicitly. The strategy is to look at the representations of $U(\mathbf{F}_q)$, the finite points of some unipotent algebraic group U, through the lens of group extensions. The strength of this methodology was quickly apparent: not only in finding results, but in providing clarity for the general case of unipotent algebraic groups.

My objective in writing this is to convince a working mathematician that the methods written here are not *a* way to study unipotent algebraic groups but that they are *the* way. Because of the efficacy of group extensions on unipotent groups, the combination of the orbit method with known extension data was completely and totally effective in analyzing two dimensional unipotent groups over perfect fields. Moreover, the obstructions to the next generalization are obvious but difficult.

Given my results, there are a couple of immediate applications. Chapter 5 is one such application. If we have a group U with certain conditions, we can build B which contains U as a normal subgroup. The representations over a not algebraically closed field ℓ are then accessible in this case while being very difficult in general. Another application is at the end of Chapter 4: a construction for inputting these groups into a computer algebra system. As a counterexample these groups have the advantage of being small by computational standards and having known representation theory.

The remainder of this thesis will by necessity be very technical and not readable by the public. To those friends, family, scientists, lawyers and business people looking to read my thesis, I encourage you to read no further.

1.1 Results

The work of Chapter 4 is to find the characters of an arbitrary two dimensional unipotent group $H = \mathbf{H}(\mathbf{F}_q)$ where $\mathbf{H}$ is an algebraic group defined over $\mathbf{F}_q$. A result in Jantzen (given here as Corollary 4.1.3) says that every extension of $\mathbf{G}_a$ by $\mathbf{G}_a$ is given by an alternating factor system β and a factor system of Witt-type ω. The chapter culminates to the following theorem, which associates a coadjoint orbit and a character using the factor system $\beta + \omega \in \operatorname{Ext}(\mathbf{G}_a, \mathbf{G}_a)$, defined over $\mathbf{F}_q$, which defines H.

Given elements $\psi_{(u,w)} \in \mathfrak{g}^*$ as defined in Theorem 4.2.5 we have the following explicit description of their coadjoint orbit $\Omega \subset \mathfrak{g}^*$ and the associated characters:

Theorem 4.2.1. *Let $\mathbf{F}_q$ be a finite field of order p^r and let $\mathbf{H}$ be an extension of $\mathbf{G}_a$ by $\mathbf{G}_a$ corresponding to the factor system $\beta+\omega$ and $H = \mathbf{H}(\mathbf{F}_q)$. Let $\alpha_1 : \mathbf{Z}/p\mathbf{Z} \to K^\times$ and $\alpha_2 : \mathbf{Z}/p^2\mathbf{Z} \to K^\times$ be choices for a primitive p-th and p^2 root of unity and let* $\operatorname{tr} = \operatorname{tr}_{\mathbf{F}_q/\mathbf{F}_p}$.

1. *If $\omega = 0$, then elements of the coadjoint orbit of $\psi_{(u,w)}$ are of the form $\psi_{(u',w)}$ and the characters of irreducible representations are given by*

$$\rho_\Omega(g_1, g_2) = \frac{1}{(\text{card } \Omega)^{1/2}} \sum_{(u,w)\in\Omega} \alpha_1 \operatorname{tr}(ug_1 + wg_2) \qquad \forall (g_1, g_2) \in H.$$

2. *If $\omega \neq 0$ then*

$$\omega(x,y) = \frac{\phi(x)^p + \phi(y)^p - (\phi(x)+\phi(y))^p}{p}.$$

Elements of the coadjoint orbit of $\psi_{(u,w)}$ are of the form $\psi_{(u,w')}$ and the characters of irreducible representations are given by $\rho_\Omega(g_1, g_2)$ which equals

$$\frac{1}{M} \sum_{(u,w)\in\Omega} \alpha_2 \operatorname{tr}(\phi(u)\phi(g_1), \phi(u)^p g_2 + \phi(g_1)^p w) \cdot \alpha_1(\operatorname{tr} g_1 u)$$

when ϕ is not an isomorphism and

$$\frac{1}{M} \sum_{(u,w)\in\Omega} \alpha_2 \operatorname{tr}(\phi(u)\phi(g_1), \phi(u)^p g_2 + \phi(g_1)^p w)$$

if ϕ *is an isomorphism for every* $(g_1, g_2) \in H_\omega$ *and* $M = (\text{card } \Omega)^{1/2}$.

Then, in Chapter 5 we find necessary and sufficient conditions expressed in terms of the cocycle $\beta + \omega$ for a torus to act on an arbitrary two dimensional unipotent group by automorphisms. If $T = \mathbf{G}_m(\mathbf{F}_q)$ and $U = H_{\beta+\omega}(\mathbf{F}_q)$ we have

Theorem 5.1.1. *Suppose* $T = \mathbf{G}_m(\mathbf{F}_q)$ *is a torus defined over* $\mathbf{F}_q$ *and that* T *acts (by* $\mathbf{F}_q$*-morphisms) on the group* U *by the rule* $t\cdot(u_1, u_2) = (t^a u_1, t^b u_2 + t^b p(u_1) - p(t^a u_1))$. *If* U *is defined by the factor system* γ *then* $\gamma + \partial p$ *is homogeneous for some polynomial* $p \in k[T]$. *If* $\gamma + \partial p$ *is homogeneous of degree* i*, then* $b = ia$. *Thus there exists a nontrivial torus action if and only if* U *is isomorphic to a group defined by a homogeneous factor system.*

With that torus action, we can build $G = U \rtimes T$ which has U as a normal subgroup. The group G is no longer a p group, so we find its representations not only over a characteristic 0 field K but over an arbitrary field κ with $\text{char}(\kappa) = \ell \neq p$. The result of Chapter 5 says that every irreducible κ-representation can be lifted from a representation of U. More precisely:

Theorem 5.2.1. *Every irreducible* κ*-representation of* G *is of the form* $\text{ind}_S^G M$ *where* M *is an irreducible representation of* S *with the form* $\text{res}_U^S M \cong W$ *for* W *an irreducible representation of* U *with stabilizer* S.

Chapter 2

Background

The fundamental object of study in this thesis is the “linear algebraic group”. The definition of a linear algebraic group pulls heavily from algebraic geometry as found in [Mum88]. The idea is to build a group which also has geometric structure as an affine variety. From there we will discuss the finite points of algebraic groups and the representations of those finite groups.

After that, we will move to a discussion of unipotent algebraic groups. We give a full treatment of relationship between cohomology and group extensions as found in [DBFPS08]. Then, we give a proof of the statement that every unipotent group is a multiple extension of additive groups. Furthermore, every unipotent group has a quotient and a subgroup which is isomorphic to $\mathbf{G}_a$.

The background information for the thesis is not constrained entirely to this chapter – other necessary information appears sporadically throughout the document. Relevant theorems related to extensions of $\mathbf{G}_a$ by $\mathbf{G}_a$ appears in Chapter 4 and representation theoretic background on Clifford theory, extendable characters and modular representations appears in Chapter 5.

2.1 Algebraic Groups

Algebraic groups are, fundamentally, groups which are algebraic varieties. There are any number of good resources for more context on varieties, we primarily use [Mum88].

We fix k an algebraically closed field. Given a set of polynomials f_i in n variables, we would like to study the locus of roots of those polynomials all at once. That locus of points has a geometry, but we can study those points with algebra.

A *closed algebraic subset* of k^n is a set consisting of all roots of a finite collection of polynomials. Such a set only depends on an ideal $\mathfrak{a} \subset k[X_1, \ldots, X_n]$ by Hilbert’s

Nullstellensatz:

Theorem 2.1.1. *Let $\mathfrak{a}$ be an ideal in $k[X_1,\ldots,X_n]$ and let Σ be a closed algebraic set. Let*

$$V(\mathfrak{a}) = \{x \in k^n \mid f(x) = 0 \quad \forall f \in \mathfrak{a}\}$$

and let

$$I(\Sigma) = \{f \in k[X_1,\ldots,X_n] \mid f(x) = 0 \quad \forall x \in \Sigma\}.$$

Then $I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$.

The Nullstellensatz gives the relationship between closed algebraic sets and ideals of $k[X_1,\ldots,X_n]$. We can make a stronger statement relating algebraic sets to k-algebras provided those k-algebras are finitely generated and reduced:

Proposition 2.1.2. *[Mum88, Proposition 1.3.2] Algebraic sets X are in bijection with finitely generated reduced k-algebras where a k-algebra is reduced if it has no non-zero nilpotent elements.*

The affine variety X corresponding to the finitely generated reduced k-algebra B is the set of maximal ideals of B. We identify that set of maximal ideals with an algebraic set by representing B as a quotient $k[X_1,\ldots,X_n]/I$ and using the Nullstellensatz to identify X with the subset $V(I)$ in $\mathbf{A}^n$. We write $k[X]$ for the k-algebra B corresponding to X.

Now, suppose that $\Sigma_1 \subset k^{n_1}$ and $\Sigma_2 \subset k^{n_2}$ are algebraic sets. We call a map $\alpha : \Sigma_1 \to \Sigma_2$ a *morphism* if it is polynomial. That is, α is defined by n_2 polynomials f_i in n_1 variables so that

$$\alpha(x) = (f_1(x_1,\ldots,x_{n_1}),\ldots,f_{n_2}(x_1,\ldots,x_{n_1})).$$

Such a morphism has a comorphism, an induced ring homomorphism on $\alpha^* : k[\Sigma_2] \to k[\Sigma_1]$ which takes $f \in k[\Sigma_2]$ to $f \circ \alpha \in k[\Sigma_1]$.

Roughly speaking, an *algebraic variety* is a topological space with a sheaf of

k-valued functions which "locally" is isomorphic to an affine variety. Further information for topological spaces with sheaves of rings can be found in [Mum88] or [Gro60].

Example 2.1.3. Let $\mathbf{A}^n$ be the algebraic set $\{x_1, \ldots, x_n | x_i \in k\}$. The set of polynomials which is 0 on the entirety of $\mathbf{A}^n$ is only the 0 polynomial. Therefore, the coordinate ring is $k[X_1, \ldots, X_n]/\langle 0 \rangle \cong k[X_1, \ldots, X_n]$. By definition, this is an affine variety. We call $\mathbf{A}^n$ *affine n-space*.

Let G be an affine variety. If G is also a group with morphisms of varieties $\mu : G \times G \to G$ and $i : x \to x^{-1}$, we call G a *linear algebraic group*. The associated algebra morphisms on $k[G]$ have names: we call $\Delta : k[G] \to k[G] \otimes k[G]$ *comultiplication* and $\iota : k[G] \to k[G]$ the *antipode*. The identity of the group is given by the *counit* $e : k[G] \to k$.

Example 2.1.4. The affine line $\mathbf{A}^1$ is an algebraic group in the following way. Suppose $k[\mathbf{A}^1] = k[T]$. We then define a comultiplication, antipode and counit.

Let comultiplication be given by

$$\Delta : T \mapsto T \otimes 1 + 1 \otimes T.$$

A choice of antipode determines a choice of counit. If the antipode is

$$\iota : T \mapsto -T + a$$

with $a \in k$ then the counit must be given by the map from $T \to k$ which takes $e : T \mapsto a$. However, as an algebraic group, this is isomorphic to the structure given by $\iota : T \mapsto -T$ and $e : T \to 0$ for any a. We try to not lose much sleep over these choices. This group is called the *additive algebraic group* and is denoted $\mathbf{G}_a$.

Products of additive groups are called *vector groups* and they give a group structure on affine n space. In fact, every unipotent algebraic group is isomorphic as a variety to $\mathbf{A}^n$ for some n. We will sketch a proof later.

A *homomorphism* of algebraic groups is a morphism of varieties which is also a group homomorphism. An *isomorphism* of algebraic groups is an isomorphism of varieties which is also a group isomorphism.

Suppose G and H are algebraic groups. A group isomorphism $\phi : G \to H$ is not necessarily an isomorphism of algebraic groups. Such a ϕ will give a bijection on the points of the underlying algebraic variety, but that bijection is not necessarily an isomorphism of varieties.

The Frobenius $\sigma : \mathbf{G}_a \to \mathbf{G}_a$ which takes $x \to x^p$ is a group isomorphism from $(k, +)$ to $(k, +)$ which is not an isomorphism of algebraic groups. The "inverse" would be the p-th root map which is not a morphism of varieties.

Any closed subgroup of GL_n is an affine variety so it is a linear algebraic group. Justification for the phrase "linear" comes from the converse which is true as well:

Theorem 2.1.5. *[Spr98, Theorem 2.3.7] Let G be a linear algebraic group. There is an isomorphism of G onto a closed subgroup of some* GL_n.

Given a linear algebraic group over a field k, we can define *F-rational points* for any subfield $F \subset k$. Given a group G which is defined over F, we call the set of F-homomorphisms $F[G] \to F$ the F-rational points of G and denote the set $G(F)$. This is the same data as F-morphisms $\mathbf{A}^0 \to G$ where $\mathbf{A}^0$ is a point.

We will be interested in the representations of the group $G(\mathbf{F}_q)$ of $\mathbf{F}_q$-rational points for certain groups G. Note that an $\mathbf{F}_q$-variety is not determined by its set of rational points.

Example 2.1.6. We compare $\mathbf{R}[T, T^{-1}]$ and $\mathbf{R}[X, Y]/\langle X^2 + Y^2 - 1\rangle$. The $\mathbf{R}$-rational points of these structures are different; the first gives the multiplicative group $\mathbf{R}^\times$ while the second gives a circle, S^1. If we extend the field to an algebraic closure $\mathbf{C}$, set $V = X + iY$ and $W = X - iY$. Then $\langle X^2 + Y^2 - 1\rangle = \langle VW - 1\rangle$ so these are both isomorphic to the algebraic group $\mathbf{G}_m$ with coordinate ring $\mathbf{C}[T, T^{-1}]$.

This demonstrates the main obstruction to working over fields which are not algebraically closed. When F is a subfield of k which is not algebraically closed, an F-variety can be extended to a different algebraic group over k. If G is a linear algebraic group defined over a field F it has coordinate ring $F[G]$. Then, the group of F rational points is

$$G(F) = \mathrm{Hom}_{F-alg}(F[G], F)$$

and for any field extension E of F we have

$$G(E) = \mathrm{Hom}_{F-alg}(F[G], E).$$

2.2 Representations of Finite Groups

Suppose that $\mathbf{G}$ is an algebraic group defined over $\mathbf{F}_q$ and that $G = \mathbf{G}(\mathbf{F}_q)$. Suppose F is an arbitrary field and V is a finite dimensional F vector space, an F-*representation* or *representation* of a finite group is a group homomorphism $\rho : G \to \mathrm{GL}(V)$. In notation we can suppress the data of ρ and call V a *G-module*. The dimension of V as a vector space is called the *dimension* of the representation. A representation is *irreducible* if it has no proper nontrivial submodules.

From a group G we can build an algebra FG by extending the product in G linearly. The *regular representation* of G is the group algebra FG, the collection of all formal sums of elements of G. The regular representation contains every irreducible G module as a submodule. An F-representation of G is the same as an FG-module. Conversely, we can restrict a representation of FG to a representation of G. The study of G-modules is in that way identical to the study of FG-modules.

Theorem 2.2.1 (Maschke)**.** *Let G be a finite group and F a field whose characteristic does not divide $|G|$. Then every FG-module is completely reducible.*

Now, suppose that ρ is a F-representation of G. The *F-character* χ of G associated to ρ is the function

$$\chi(g) = \mathrm{tr}\,\rho(g).$$

Not only are characters class functions $G \to F$, but for any sufficiently large field F of characteristic not dividing $|G|$ the characters span the space of class functions. Related to that, over a sufficiently nice field the characters of an abelian group are all 1-dimensional. The F-vector space of class functions on G has a non-degenerate inner product defined by the rule

$$\langle \chi, \theta \rangle = \sum_{g \in G} \chi(g)\theta(g^{-1}).$$

Suppose that $H \subset G$. A FG-module V is a FH-module $\operatorname{res}_H^G V$ which we call the *restriction*. A FH-module W can similarly be *induced* to G by $\operatorname{ind}_H^G W = FG \otimes_{FH} W$. We have a relationship between induced modules and restricted modules by *Frobenius Reciprocity*

Lemma 2.2.2 (Frobenius Reciprocity)**.** *[CR06, Theorem 10.8] Let $H \leq G$ and let L be a left FH-module and M a left FG-module. Then there exists an isomorphism of F-modules*

$$\operatorname{Hom}_{FH}(L, \operatorname{res}_H^G M) \cong \operatorname{Hom}_{FG}(\operatorname{ind}_H^G L, M).$$

We can induce or restrict characters by inducing or restricting the associated module. Frobenius Reciprocity can also be stated for class functions as:

Lemma 2.2.3. *[CR06, Theorem 10.9] Let $H \subset G$ and suppose that ϕ is a class function on H and that θ is a class function on G. Then*

$$\langle \phi, \operatorname{res}_H^G \theta \rangle = \langle \operatorname{ind}_H^G \phi, \theta \rangle.$$

2.3 Unipotent Algebraic Groups

Suppose V is a finite dimensional k-vector space. An endomorphism n of V is *nilpotent* if $n^s = 0$ for some positive integer s. An endomorphism u is *unipotent* if $u - 1$ is nilpotent. Since k has characteristic p, u is unipotent if and only if $u^{p^i} = 1$ for some integer i. We call a linear algebraic group unipotent if every element is unipotent. The following two statements from [Spr98] give a characterization which justifies the nomenclature.

Proposition 2.3.1. *[Spr98, Proposition 2.4.12] Let G be a subgroup of GL_n consisting of unipotent matrices. There is $x \in \mathrm{GL}_n$ such that $xGx^{-1} \subset U_n$, the group of upper triangular matrices with 1 on the diagonal.*

Corollary 2.3.2. *[Spr98, Corollary 2.4.13] A unipotent linear algebraic group is nilpotent, hence solvable.*

An *isogeny* is a surjective homomorphism of algebraic groups with finite kernel. In positive characteristic, interesting isogenies arise as a result of the Frobenius morphism. As an example, consider $x^p - x \in \mathrm{Hom}(\mathbf{G}_a, \mathbf{G}_a)$. This is called the *Lang-isogeny* and it is surjective when k is an algebraic closure of $\mathbf{F}_p$. Isogenies will play a fundamental role in the classification of connected commutative unipotent groups.

Now, let A and B be connected unipotent k groups and let A be commutative. An *extension of B by A* is a group C so that

$$0 \longrightarrow A \xrightarrow{i} C \xrightarrow{\pi} B \longrightarrow 1$$

with maps i and π is an exact sequence. We usually refer to an extension without explicitly mentioning i and π, but technically all three are part of the data of the extension.

We call a morphism of algebraic varieties $f : B \times B \to A$ a *factor system* if it satisfies

$$f(a,b) + f(ab,c) - f(b,c) - f(a,bc) = 0. \tag{2.1}$$

A factor system is sufficient to define the extension of groups

$$0 \longrightarrow A \longrightarrow C \longrightarrow B \longrightarrow 1$$

where A is central in C. We can define the operation on C given a fixed f. We construct $C \cong B \times A$ as a variety with group operation given by

$$(b_1, a_1)(b_2, a_2) = (b_1 b_2, a_1 + a_2 + f(b_1, b_2)).$$

One can immediately check that the factor system condition is exactly equivalent to checking that this group operation is associative.

Given an extension C determined by the factor system f, we have a section

$s : B \to C$ given by $s(b) = (b, 1)$. In a similar way, if there exists a section $s : B \to C$ then there exists a factor system $\beta : B \times B \to C$. One can take

$$\beta(b_1, b_2) = i^{-1}(s(b_1 b_2)s(b_1^{-1})s(b_2^{-1})).$$

Given such a section, the ordered pair from the previous paragraph is exactly $i(a)s(b)$.

However, existence of such a section (equivalently, a factor system) is nontrivial. We will show in Subsection 2.3.1 that every unipotent group over a perfect field is a multiple extension of additive groups.

Let $f : A \to A'$ be a homomorphism. The *pushforward* of f is the unique extension $f_*(C)$ so that there exists a homomorphism $F : C \to f_*(C)$ which makes the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & C & \longrightarrow & B & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle F} & & \downarrow{\scriptstyle id} & & \\ 0 & \longrightarrow & A' & \longrightarrow & f_*(C) & \longrightarrow & B & \longrightarrow & 0 \end{array}$$

commute. Similarly, for a homomorphism $g : B' \to B$ the *pullback* of g is the unique extension $g^*(C)$ so that there exists a homomorphism F which makes the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & g^*(C) & \longrightarrow & B' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle F} & & \downarrow{\scriptstyle g} & & \\ 0 & \longrightarrow & A & \longrightarrow & C & \longrightarrow & B & \longrightarrow & 0 \end{array}$$

commute. The pushforward and pullback are notated fC and Cg. Two extensions H_1 and H_2 are isomorphic as extensions if there exists an isomorphism $\phi : H_1 \to H_2$ which makes the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & H_1 & \longrightarrow & B & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle id} & & \\ 0 & \longrightarrow & A & \longrightarrow & H_2 & \longrightarrow & B & \longrightarrow & 0 \end{array}$$

commute. A morphism $g : B \to A$ with $\delta g : B \times B \to A$ given by $\delta g(b_1, b_2) = g(b_1 b_2) - g(b_1) - g(b_2)$ yields exactly such a map. The isomorphism ϕ associated to

g takes (b_1, a_1) in H_1 to $(g(b_1), a_1)$ and if C has factor system f, the isomorphism implies H_2 has the factor system $f + \delta g$. We call factor systems which are δg for some g *trivial*.

We can compare factor systems to cohomological data from the Hochschild complex from [Jan03].

Definition 2.3.3. [Jan03, Section 4.14] Let G be an algebraic group and let M be a G module. The chain complex $C^*(G, M)$ has $C^n(G, M) = M \otimes \bigotimes^n k[G]$ with boundary maps from C^n to C^{n+1} by $\partial^n = \sum_{i=0}^{n+1}(-1)^i \partial_i^n$ where

$$\begin{aligned}
\partial_0^n(m \otimes f_1 \otimes \cdots \otimes f_n) &= \Delta_M(m) \otimes f_1 \otimes \cdots \otimes f_n \\
\partial_i^n(m \otimes f_1 \otimes \cdots \otimes f_n) &= m \otimes f_1 \otimes \cdots \otimes f_{i-1} \otimes \Delta_G(f_i) \otimes \cdots \otimes f_n \\
\partial_{n+1}^n(m \otimes f_1 \otimes \cdots \otimes f_n) &= m \otimes f_1 \otimes \cdots \otimes f_n \otimes 1.
\end{aligned}$$

The chain complex $C^*(G, M)$ is called the *Hochschild Complex*.

Each $C^n(G, M)$ can be interpreted as morphisms $G^n \to M$. In that way, the image of C^1 in C^2 under ∂^1 are trivial factor systems: ∂^1 takes

$$\begin{aligned}
\partial^1(m \otimes f_1) &= \Delta_M(m) \otimes f_1 - m \otimes \Delta_G(f_1) + m \otimes f_1 \otimes 1 \\
&= m \otimes 1 \otimes f_1 + m \otimes f_1 \otimes 1 - m \otimes \Delta_G(f_1)
\end{aligned}$$

which are exactly the maps $f(a) + f(b) - f(ab)$ from $G \times G \to M$, the trivial factor systems. We similarly have that the kernel of C^2 under ∂^2 are all factor systems $G \times G \to M$. This gives a bijection between isomorphic classes of extensions of B by A and $H^2(B, A)$.

There exists a theory of cohomology of abstract groups with the same cocycle condition 2.1 where it is not required factor systems are morphisms of varieties. This gives a different notion of group cohomology than the one given.

2.3.1 Unipotent groups as extensions

For the remainder of this chapter until Chapter 4 we no longer require that k be algebraically closed and instead ask that it be perfect. We now show that every connected unipotent group over a perfect field k is a multiple extension of groups of the type $\mathbf{G}_a(k)$ following the argument from [McN10, Section 2.2]. A connected unipotent linear group U is *k-split* if there is a sequence of closed, connected normal subgroups of U

$$1 = U_m \subset U_{m-1} \subset \cdots \subset U_1 \subset U_0 = U$$

so that each quotient is isomorphic to $\mathbf{G}_a$. By [Spr98, Corollary 14.3.10] every connected unipotent group over a perfect field is k-split.

Proposition 2.3.4. *[Spr98, Theorem 14.2.6] as in [McN10] Suppose that the linear algebraic group G has a normal, connected, k-split unipotent subgroup R. Then there is a morphism of k-varieties $s : G/R \to G$ which is a section to $\pi : G \to G/R$.*

This follows essentially from a result widely attributed to Rosenlicht as written in [Ros56]. Now, suppose U is defined over an algebraically closed field. Then there is an exact sequence

$$1 \longrightarrow U_{i+1} \xrightarrow{i} U_i \xrightarrow{\pi} \mathbf{G}_a \longrightarrow 0$$

with a section $s : \mathbf{G}_a \to U_i$. Therefore, there is a factor system $\mathbf{G}_a \times \mathbf{G}_a \to U_{i+1}$ which defines an extension of $\mathbf{G}_a$ by U_{i+1}. As a corollary,

Corollary 2.3.5. *[Spr98, 14.2.7] If G is k-split it is isomorphic as a k-variety to $\mathbf{A}^n$.*

On the other hand,

Theorem 2.3.6. *[Spr98, Lemma 14.39] Every k-split group has a closed normal central subgroup N that is isomorphic to $\mathbf{G}_a$.*

Therefore, every U_i has a normal subgroup $\mathbf{G}_a$ and the sequence

$$0 \longrightarrow \mathbf{G}_a \xrightarrow{i} U_i \xrightarrow{\pi} U_i/\mathbf{G}_a \longrightarrow 1$$

also has a section by Proposition 2.3.4. This defines an extension of $U/\mathbf{G}_a$ by $\mathbf{G}_a$. Since $U_i/\mathbf{G}_a$ is a unipotent group of dimension strictly less than U_i, every unipotent group is a repeated central extension of additive groups. Furthermore, every unipotent algebraic group has a quotient which is isomorphic to $\mathbf{G}_a$ and a subgroup isomorphic to $\mathbf{G}_a$.

Chapter 3

Commutative Unipotent Groups

Let k be a perfect field of characteristic p. Over k, the Witt ring is also a unipotent linear algebraic group. Products of Witt vectors play a structural role in the theory of commutative unipotent algebraic groups by theorems in *Algebraic Groups and Class Fields* [Ser88] and recalled here as Theorem 3.1.5. The first section deals with the definitions of the Witt ring, truncated Witt vectors and their structure as group extensions. Since they are commutative groups, their irreducible representations over finite fields are not complicated but they play a large role in the following chapters. The material of Section 3.1 is from [Ser79] and [Ser88] with some perspectives from [McN02] and [DBFPS08].

The second section gives definitions for perfectization, as found in [BD06] and [Gre65]. From those definitions and the arguments [Ser88] we construct the analogue of Theorem 3.1.5 for perfect unipotent group schemes.

3.1 Witt Vectors

Let $(X_0, X_1, X_2, \ldots)$ and $(Y_0, Y_1, Y_2, \ldots)$ be two sequences of indeterminants. Given a prime number p the *Witt Polynomials* are given by

$$\begin{aligned} W^0 &= X_0 \\ W^1 &= pX_1 + X_0^p \\ W^2 &= p^2 X_2 + pX_1^p + X_0^{p^2} \\ &\vdots \\ W^n &= \sum_{i=0}^{n} p^i X_i^{p^{n-i}} \end{aligned}$$

Theorem 3.1.1 (Witt). *For every $\Phi \in \mathbf{Z}[X, Y]$, there exists a unique sequence*

$(\phi_0, \ldots, \phi_n, \ldots)$ *of elements in* $\mathbf{Z}[X_0, Y_0, X_1, Y_2, \ldots, X_n, Y_n, \ldots]$ *so that*

$$W^n(\phi_0, \ldots, \phi_n, \ldots) = \Phi(W^n(X_0, \ldots, X_n, \ldots), W^n(Y_0, \ldots, Y_n, \ldots))$$

for all n.

We are interested primarily in $\Phi(X, Y) = X + Y$ and $\Phi(X, Y) = XY$. Given $\Phi(X, Y) = X + Y$, the theorem says that we can define "internal" polynomials ϕ_i so that

$$W^n(X) + W^n(Y) = W^n(\phi_0, \ldots, \phi_n)$$

for each n. We call $\phi_i = S_i$ for addition and $\phi_i = P_i$ for multiplication. Example 3.1.2 gives the first three S_i and P_i.

Since we can add and multiply elements, we can build rings from elements in an arbitrary commutative ring A. Given two infinite sequences in A, $a = (a_0, \ldots, a_n, \ldots)$ and $b = (b_0, \ldots, b_n, \ldots)$ the ring structure is given by

$$a + b = (S_0(a, b), \ldots, S_n(a, b), \ldots)$$

and

$$ab = (P_0(a, b), \ldots, P_n(a, b), \ldots).$$

We call this the "ring of Witt vectors with coefficients in A".

For the remainder of this thesis, we will only concern ourselves with truncated Witt vectors. Since S_i and P_i contain only variables of index $\leq i$, we can consider Witt vectors of finite length. If the shift operator $V : W(A) \to W(A)$ takes

$$(a_0, a_1, \ldots) \mapsto (0, a_0, a_1, \ldots)$$

we call

$$W_n(A) = \frac{W(A)}{V^n W(A)}.$$

The sets of $(a_0, \ldots, a_{n-1})$ are called "truncated Witt vectors". Notice that the $W_i(A)$

are rings as opposed to the super-scripted W^j which were polynomials. When there is no ambiguity about A we will denote the truncated Witt vectors of length n by W_n. For the remainder of this thesis, we will only concern ourselves with truncated Witt vectors.

The Witt vectors and truncated Witt vectors are a generalization of the p-adic integers. When $A = \mathbf{F}_p$ the Witt ring is isomorphic to the p-adic integers and the truncated Witt ring has $W_n(\mathbf{F}_p) \cong \mathbf{Z}/p^n\mathbf{Z}$.

Example 3.1.2. We construct the Witt vectors over k of length 3. Let $x = (x_0, x_1, x_2)$ and $y = (y_0, y_1, y_2)$ be two elements of W_3. We have

$$S_0(x,y) = x_0 + y_0$$
$$S_1(x,y) = x_1 + y_1 + \frac{x_0^p + y_0^p - (x_0 + y_0)^p}{p}$$
$$S_2(x,y) = x_2 + y_2 + \frac{x_1^p + y_1^p - S_1(x,y)^p}{p} + \frac{x_0^{p^2} + y_0^{p^2} - (x_0 + y_0)^{p^2}}{p^2}$$

As a warning, it might be tempting to claim that $S_1(x,y)$ is $x_1 + y_1 + 0$ because $(x+y)^p = x^p + y^p$ modulo p. That is explicitly not the case. Every coefficient of $(x_0 + y_0)^p$ other than x_0^p and y_0^p is divisible by p, so the polynomial $S_1(x,y)$ gives all of the terms which are 0 modulo p.

It is also worth mentioning that there are terms in $S_1(x,y)/p$ that have p^2 in the denominator. Such terms are not only necessary by construction, but necessary to give S_2 integer coefficients since the term

$$\frac{x_0^{p^2} + y_0^{p^2} - (x_0 + y_0)^{p^2}}{p^2}$$

does not have coefficients in $\mathbf{Z}$.

We also have interesting p interactions with multiplication. We compute

$$P_0(x,y) = x_0 y_0$$

$$P_1(x,y) = y_0^p x_1 + x_0^p y_1 + p x_1 y_1$$

$$P_2(x,y) = x_2 y_0^{p^2} + x_1^p y_1^p + y_2 x_0^{p^2} + p(x_2 y_1^p + y_2 x_1^p) + \\ + p^2 x_2 y_2 + \frac{x_1^p y_0^{p^2} + y_1^p x_0^{p^2} - P_1(x,y)^p}{p}.$$

In k, when the leading coefficient is p or p^2, it is 0 so our multiplication functions are actually:

$$P_0(x,y) = x_0 y_0$$

$$P_1(x,y) = y_0^p x_1 + x_0^p y_1$$

$$P_2(x,y) = x_2 y_0^{p^2} + x_1^p + y_1^p + y_2 x_0^{p^2} + \frac{x_1^p y_0^{p^2} + y_1^p x_0^{p^2} - P_1(x,y)^p}{p}.$$

3.1.1 Witt Vectors as Group Extensions

Let k be an algebraically closed field of characteristic p and let $W_n = W_n(k)$ for all n. The groups W_n and W_m have three operations which connect them.

1. $F : W_n \to W_n$ which takes $(x_0, \ldots, x_{n-1})$ to $(x_0^p, \ldots, x_{n-1}^p)$ is called the Frobenius homomorphism.

2. $V : W_n \to W_{n+1}$ which takes $(x_0, \ldots, x_{n-1})$ to $(0, x_0, \ldots, x_{n-1})$ is called the shift homomorphism.

3. $R : W_{n+1} \to W_n$ which takes $(x_0, \ldots, x_{n-1}, x_n)$ to $(x_0, \ldots, x_{n-1})$ is called the restriction homomorphism.

All three operations commute with each other. We can in general make the strictly exact sequence

$$0 \longrightarrow W_n \xrightarrow{V^n} W_{n+m} \xrightarrow{R^m} W_n \longrightarrow 0.$$

Given commutative algebraic groups A and B one can define a group $\text{Ext}(A, B)$ of commutative extensions of A by B as in [Ser88, VII Section 1]. Then $\text{Ext}(W_n, W_m)$ refers to the commutative extensions of W_n by W_m. We find the element of $\text{Ext}(\mathbf{G}_a, \mathbf{G}_a)$

corresponding to the extension

$$0 \longrightarrow \mathbf{G}_a \xrightarrow{V} W_2 \xrightarrow{R} \mathbf{G}_a \longrightarrow 0\ .$$

Given R, there exists a section $s : \mathbf{G}_a \to W_2$ which has $s(x) = (x, 0)$. Any section gives a factor system $\omega(x,y) = s(x) + s(y) - s(x+y)$. That factor system in this case gives a rule for addition in W_2, we have

$$\omega(x,y) = \frac{x^p + y^p - (x+y)^p}{p}.$$

From that, we can talk about the left and right module structure of $\mathrm{Ext}(\mathbf{G}_a, \mathbf{G}_a)$ in terms of ω.

Example 3.1.3. Let $\phi \in \mathrm{Hom}(\mathbf{G}_a, \mathbf{G}_a)$. Then $\phi(x)$ is a polynomial in p-th powers of x

$$\phi(x) = \sum a_i x^{p^i}.$$

We want to compare the extension $\phi\alpha_1^1$ with $\alpha_1^1\phi$. That is, we would like to know the difference between

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbf{G}_a & \xrightarrow{V} & W_2 & \xrightarrow{R} & \mathbf{G}_a & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi} & & \downarrow & & \downarrow{\scriptstyle id} & & \\ 0 & \longrightarrow & \mathbf{G}_a & \longrightarrow & H & \longrightarrow & \mathbf{G}_a & \longrightarrow & 0 \end{array}$$

and

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbf{G}_a & \longrightarrow & K & \longrightarrow & \mathbf{G}_a & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle id} & & \downarrow & & \downarrow{\scriptstyle \phi} & & \\ 0 & \longrightarrow & \mathbf{G}_a & \xrightarrow{V} & W_2 & \xrightarrow{R} & \mathbf{G}_a & \longrightarrow & 0. \end{array}$$

Composition on the left gives us p-th powers of the factor system ω, we have $\phi\alpha_1^1 = \sum a_i \omega^{p^i}$. This corresponds to applying ϕ to the copy of $\mathbf{G}_a$ in the center of W_2. The factor system corresponding to H is $\phi(\omega(x,y))$. However, if we apply ϕ to the right, that copy of $\mathbf{G}_a$ is not central. It means that K corresponds to the factor system

$\omega(\phi(x), \phi(y))$. The factor system ω is not additive, but it does commute with the Frobenius. Therefore we have $\alpha_1^1 \phi = \sum a_i^p \omega$.

Proposition 3.1.4. *[Ser88, VII Proposition 10] Let $W = \prod W_{n_i}$ be a product of Witt groups, and let G be a connected unipotent group. The following conditions are equivalent:*

1. *There exists an isogeny $f : G \to W$.*

2. *There exists an isogeny $g : W \to G$.*

When these conditions hold, we call W and G isogenous.

The following theorem gives a complete classification of connected unipotent groups.

Theorem 3.1.5. *[Ser88, VII Theorem 1-3] Every commutative connected unipotent group is isogenous to a product of Witt groups, isomorphic to a subgroup of a product of Witt groups, and isomorphic to a quotient of a product of Witt groups by a connected subgroup.*

3.1.2 Representations of Commutative Unipotent Groups

Let $q = p^r$. The trace $\mathrm{tr}_{\mathbf{F}_q/\mathbf{F}_p}$ is the sum of the elements of the Galois group of $\mathbf{F}_q$ over $\mathbf{F}_p$. Since the map is fixed by every element of the Galois group, the trace takes elements of $\mathbf{F}_q$ to elements of $\mathbf{F}_p$. It is also the trace of the $r \times r$ matrix with entries in $\mathbf{F}_p$ which gives multiplication by an element $x \in \mathbf{F}_q$.

The elements $\sigma \in \mathrm{Gal}(\mathbf{F}_q/\mathbf{F}_p)$ can be extended to act on the $\mathbf{F}_q$-points of affine n-space by

$$\sigma \cdot (x_1, \ldots, x_n) = (\sigma x_1, \ldots, \sigma x_n).$$

This allows us to define a trace morphism on Witt vectors by

$$\mathrm{tr}_{\mathbf{F}_q/\mathbf{F}_p} : W_n(\mathbf{F}_q) \to W_n(\mathbf{F}_q)$$

is given by

$$\mathrm{tr}_{\mathbf{F}_q/\mathbf{F}_p}(x) = F^r(x) + F^{r-1}(x) + \cdots + F(x)$$

with addition in $W_n(\mathbf{F}_q)$. We can see that $\sigma \cdot \mathrm{tr}_{\mathbf{F}_q/\mathbf{F}_p}(x) = \mathrm{tr}_{\mathbf{F}_q/\mathbf{F}_p}$ for every element $\sigma \in \mathrm{Gal}(\mathbf{F}_q/\mathbf{F}_p)$. Thus the trace defines a morphism

$$\mathrm{tr}_{\mathbf{F}_q/\mathbf{F}_p} : W_n(\mathbf{F}_q) \to W_n(\mathbf{F}_p).$$

Now, we find the $\mathbf{C}$ representations (sometimes called *ordinary*) representations of Witt vectors. To find irreducible representations, we first need to fix a root of unity in $\mathbf{C}^\times$. In particular, for Witt vectors of length n, we will need to fix a primitive p^n-th root of unity. We cannot choose such a root canonically, but we will in general fix a group homomorphism $\alpha_n : \mathbf{Z}/p^n\mathbf{Z} \to \mathbf{C}^\times$ and write all representations of a given group in terms of α_n.

Lemma 3.1.6. *Let G be a finite group with ρ a nontrivial irreducible character. Then*

$$\sum_{g \in G} \rho(g) = 0.$$

Proof. Let 1_G be the trivial character of G. Since ρ is nontrivial and irreducible, $\langle \rho, 1_G \rangle = 0$. □

Lemma 3.1.7. *Let $\mathbf{F}_q$ be a finite field of size p^r. The irreducible representations of $W_n(\mathbf{F}_q)$ are in bijection with elements of $W_n(\mathbf{F}_q)$. In particular, given an element $x \in W_n(\mathbf{F}_q)$, the map $\phi_x : G \to \mathbf{C}$ given by*

$$\phi_x(y) = \alpha_n(tr_{\mathbf{F}_q/\mathbf{F}_p} xy)$$

is an irreducible character and not isomorphic to ϕ_y when $x \neq y$.

Proof. Since W_n is a commutative group, the first part follows immediately. Now fix $\alpha_n : \mathbf{Z}/p^n\mathbf{Z} \to \mathbf{C}^\times$ a choice of a primitive p^n-th root of unity. The trace map is a homomorphism which sends an element of $W(\mathbf{F}_q)$ to $\mathbf{Z}/p^n\mathbf{Z}$. Therefore, the map

$\phi_x(y) = \alpha_n(\mathrm{tr}_{\mathbf{F}_q/\mathbf{F}_p}\, xy)$ is necessarily an irreducible representation; the only question is if it is unique.

Suppose $x \neq y$ in W_n. We check that $\langle \phi_x, \phi_y \rangle = 0$. Indeed

$$\langle \phi_x, \phi_y \rangle = \frac{1}{|W_n|} \sum_{g \in W_n} \alpha_n(\mathrm{tr}_{\mathbf{F}_q/\mathbf{F}_p}\, xg)\alpha_n(\mathrm{tr}_{\mathbf{F}_q/\mathbf{F}_p} -yg).$$

Since both α_n and $\mathrm{tr}_{\mathbf{F}_q/\mathbf{F}_p}$ are homomorphisms, this simplifies to

$$\sum_{g \in W_n} \alpha_n(\mathrm{tr}_{\mathbf{F}_q/\mathbf{F}_p}\, g(x-y)).$$

Since $x - y \neq 0$, this is ϕ_{x-y}, a nontrivial character of W_n. Therefore, by Lemma 3.1.6, $\langle \phi_x, \phi_y \rangle = 0$ so ϕ_x and ϕ_y are distinct. Therefore, every representation of W_n is of this form. □

Theorem 3.1.8. *Suppose G is an arbitrary connected commutative unipotent group and suppose G is a subgroup of a product of Witt groups $W = V_1 \oplus \cdots \oplus V_m$. The irreducible representations of G are of the form*

$$\phi_{x_1} \boxtimes \cdots \boxtimes \phi_{x_m}$$

where x_i is an element of V_i.

Proof. Suppose G is an arbitrary connected commutative unipotent group which is a subgroup of $W = V_1 \oplus \cdots \oplus V_m$ a product of Witt groups given by $i : G \to W$. The irreducible representations of V_i are given as ϕ_x for $x \in V_i$ by Lemma 3.1.7.

Let H be a subgroup of V_i. The restriction of the irreducible representations of V_i to H are also irreducible, since they are one dimensional. Since every irreducible representation of H occurs this way, the theorem follows. □

3.2 Perfectization of Abelian Unipotent Groups

In order to define a group scheme, we must first define k-group functors as in [Jan03, Section 2.1] for an arbitrary field k. In many cases Linear Algebraic Groups are exactly the same as Affine Group Schemes. For any k-algebra R the k-functor $\mathrm{Spec}_k(R)$ takes a k-algebra A to the set of every k-algebra homomorphism from R to A. The functor takes morphisms

$$\mathrm{Spec}_k(R)(\phi) : \mathrm{Hom}(R, A) \to \mathrm{Hom}(R, A') \qquad \alpha \mapsto \phi \circ \alpha.$$

Any k-functor which is isomorphic to a $\mathrm{Spec}_k(R)$ is called an *affine scheme*. For any k-functor X we denote $\mathrm{Mor}(X, \mathbf{A}^1)$ by $k[X]$.

Let X be an affine scheme over any field k. We call X *algebraic* if $k[X] \cong k[T_1, \dots, T_n]/I$ for a finitely generated ideal I of $k[T_1, \dots, T_n]$. A *k-group functor* is a functor from the category of all k-algebras to the category of groups. Then, an *algebraic k-group* is a k-group functor which is an algebraic scheme over k when seen as a k-functor.

Now, for a k-group functor the group structure determines morphisms of k-functors which correspond to multiplication, the identity and the inverse. We immediately then have comorphisms Δ (comultiplication), e (counit) and ι (the antipode).

Compare the following example to Example 2.1.4:

Example 3.2.1. Let k be an algebraically closed field. Then $\mathbf{G}_a$ is the k-group functor which takes all k-algebras A to the group of A under addition. In particular, $\mathbf{G}_a(k) = k$ as an additive group. We then have $k[\mathbf{G}_a] \cong k[T]$ which means that $\mathbf{G}_a$ is algebraic. This gives that $\mathbf{G}_a$ is a k-group functor.

Now let k be a perfect field. A *perfect* k-scheme is a scheme on which the absolute Frobenius morphism is an isomorphism. There exists a functor which takes an arbitrary k-scheme to a perfect k-scheme. Theorem 3.1.5 shows that every connected unipotent group is isomorphic to a subgroup of a product of Witt groups. A reasonable question is if perfectized Witt vectors also contain the structure of all connected perfect group schemes in a similar way. Using a close analogue of Serre's construction, we show that they do. This work follows the argument made by Serre in [Ser88].

Let S be a scheme. The *absolute Frobenius morphism* on S is the morphism which is the identity on the underlying topological space on S and the map $f \mapsto f^p$ on local sections of the structure sheaf $\mathcal{O}_S$. We call S *perfect* if the absolute Frobenius morphism $\Phi_{S,p} : S \to S$ is an isomorphism. The notion of a perfectization functor was introduced by Greenberg in [Gre65], but we follow the construction in [BD06] instead.

Define Sch_p to be the category of $\mathbf{F}_p$-schemes. Then there's a full subcategory of Sch_p of perfect $\mathbf{F}_p$ schemes, which we will call $\mathrm{Sch}_p^{\mathrm{perf}}$. The embedding of $\mathrm{Sch}_p^{\mathrm{perf}} \hookrightarrow \mathrm{Sch}_p$ has a right adjoint,

$$\mathrm{Sch}_p \to \mathrm{Sch}_p^{\mathrm{perf}}$$

which takes

$$S \mapsto S^{\mathrm{perf}}$$

which we call the *perfectization functor*.

Topologically S^{perf} is exactly the same as S, but the structure sheaf is the direct limit of the structure sheaf under $\Phi_{S,p}^*$.

For any perfect field k of characteristic $p > 0$ we say that a k-scheme is perfect if it is perfect as an $\mathbf{F}_p$ scheme. A *perfect group scheme over* k is a group object in the category of perfect k-schemes. However, since we often begin with algebraic groups, it is generally preferable to use that they are the image of an algebraic group under the perfectization functor. The following example is instructive:

Example 3.2.2. Let $G = \mathbf{G}_a$ over k a field of characteristic p. The coordinate ring of $\mathbf{G}_a$ is $k[T]$. We apply the perfectization functor to $\mathbf{G}_a$ to get $\mathbf{G}_a^{\mathrm{perf}}$, the perfect group scheme given by the direct limit of the Frobenius.

Similar to the notation for a perfect scheme, we will write the associated resulting ring with a superscript "perf". In $k[T]^{\mathrm{perf}}$ we have a q-th root of T for every $q = p^r$. That is, for every power of the Frobenius we have the inverse map in the coordinate ring of the perfectized $\mathbf{G}_a$.

As a remark, even though $\mathbf{G}_a$ was a linear algebraic group, $\mathbf{G}_a^{\mathrm{perf}}$ is not. Since $k[T]^{\mathrm{perf}}$ is not Noetherian, $\mathbf{G}_a^{\mathrm{perf}}$ is not affine.

In W_n^{perf}, the additive and multiplicative structure are exactly the same as W_n.

That is, if x and y are in W_n^{perf} we have

$$x + y = (S_1(x_1, y_1), S_2(x_2, y_2, x_1, y_1), \dots, S_n(x_n, y_n, \dots, x_1, y_1))$$

and

$$x.y = (P_1(x_1, y_1), P_2(x_2, y_2, x_1, y_1), \dots, P_n(x_n, y_n, \dots, x_1, y_1)).$$

The argument for Theorem 3.1.5 in *Algebraic Groups and Class Fields* follows from making an observation about the module structure of $H^2(\mathbf{G}_a, \mathbf{G}_a)$. By making the corresponding observation about $H^2(\mathbf{G}_a^{\text{perf}}, \mathbf{G}_a^{\text{perf}})$, the remainder of the argument will follow in a straightforward way.

Proposition 3.2.3. *$H^2_{reg}(\mathbf{G}_a^{\text{perf}}, \mathbf{G}_a^{\text{perf}})$ admits a basis of p^i-th powers of the factor system*

$$F(x, y) = \frac{1}{p}(x^p + y^p - (x + y)^p)$$

where $i \in \mathbb{Z}$.

Proof. First, note that every p^i-th power of $F(x, y)$ is necessarily a representative for a class of regular symmetric factor systems in $H^2_{reg}(\mathbf{G}_a^{\text{perf}}, \mathbf{G}_a^{\text{perf}})$. These are linearly independent.

Let $G(x, y)$ be a regular symmetric factor system in $H^2_{reg}(\mathbf{G}_a^{\text{perf}}, \mathbf{G}_a^{\text{perf}})$. Since the regular functions on $\mathbf{G}_a^{\text{perf}}$ are polynomials and p-th roots, let i be the largest integer for which $x^{p^{-i}}$ appears in $G(x, y)$. Then $G(x, y)^{p^i}$ is a polynomial, and it is also necessarily a regular symmetric factor system for $H^2_{reg}(\mathbf{G}_a, \mathbf{G}_a)$. By [Ser88, VII Proposition 8] $H^2(\mathbf{G}_a, \mathbf{G}_a)_s$ admits a basis for the p^i-th powers of the factor system F.

Thus $G(x, y)^{p^i}$ is in the span of p^j-th powers of $F(x, y)$ for j a *positive* integer which means that $G(x, y)$ is in the span of p^k-th powers of $F(x, y)$ for $k \in \mathbf{Z}$.

□

Lemma 3.2.4. *Every element $x \in \operatorname{Ext}(\mathbf{G}_a^{\text{perf}}, \mathbf{G}_a^{\text{perf}})$ can be written uniquely as $x = \phi\alpha_1^1$ and as $x = \alpha_1^1\psi$ with $\phi, \psi \in A_1$.*

Proof. We know that α_1^1 corresponds to F. According to Proposition 3.2.3, x corresponds to the factor system of the form

$$f = \sum_{i=-m}^{n} a_i F^{p^i}.$$

On the other hand, every endomorphism in A_1 can be written uniquely in the form

$$\phi(t) = \sum b_i t^{p^i}.$$

Thus $x = \phi\alpha_1^1$ if and only if $b_i = a_i$ for all i. Similarly, if

$$\psi(t) = \sum c_i t^i$$

we have $x = \alpha_1^1\psi$ with $c_i^p = a_i$. □

The remainder of the lemmas used to prove Theorem 3.2.5 and Theorem 3.2.6 follow from the associated lemmas in [Ser88]. The details of those modified proofs are slightly modified relative to their Serre counterparts, and are in Appendix A for completeness. Once the details are checked we have the following two theorems:

Theorem 3.2.5. *Every commutative connected unipotent perfect group scheme is isogenous to a product of perfect Witt group schemes.*

Proof. See A.1. □

Theorem 3.2.6. *Every commutative connected perfect unipotent group scheme is isomorphic to a subgroup of a product of perfect Witt groups and isomorphic to a quotient of a product of perfect Witt groups by a connected subgroup.*

Proof. See A.1. □

Chapter 4

Two Dimensional Unipotent Groups

4.1 Mechanisms

Let k be an algebraically closed field of characteristic $p > 2$ and let $\mathbf{G}_a$ be the additive group. A central extension

$$0 \longrightarrow \mathbf{G}_a \longrightarrow \mathbf{H} \longrightarrow \mathbf{G}_a \longrightarrow 0$$

can be described by an element α in $H^2(\mathbf{G}_a, k)$ by in Section 2.3. When $\mathbf{H}$ is defined over $\mathbf{F}_q$, this chapter gives a procedure for finding irreducible characters of the group of points $H = \mathbf{H}(\mathbf{F}_q)$ using the cohomology class α.

We describe $H^1(\mathbf{G}_a, k)$ and $H^2(\mathbf{G}_a, k)$, the first and second rational group cohomology using the Hochschild complex as recounted in Definition 2.3.3. Let k be an algebraically closed field of characteristic > 2 and suppose V_a is a k-vector space of finite rank with the ring $k[T_1, \ldots, T_n]$ of polynomial functions on V_a.

Lemma 4.1.1. *[Jan03, Lemma 4.21] If* $\operatorname{char}(k) = p \neq 0$ *then*

$$H^1(V_a, k) = \sum_{i=1}^{n} \sum_{r=0}^{\infty} kT_i^{p^r}.$$

These give the additive polynomials as found in Section 3.3 of [Spr98]. Next, we need to develop the elements which correspond to the truncated Witt vectors of length 2. First, we define

$$\begin{Bmatrix} p \\ i \end{Bmatrix} := \frac{1}{p} \begin{pmatrix} p \\ i \end{pmatrix}$$

and notice that it is an integer for all $0 < i < p$. Then, for $f \in k[V_a]$, define

$$\omega(f) = \sum_{i=1}^{p-1} \begin{Bmatrix} p \\ i \end{Bmatrix} f^i \otimes f^{p-i}$$

and let $\bar{\omega}$ be the induced map $\bar{\omega} : H^1(V_a, k) \to H^2(V_a, k)$. Jantzen again gives us the following crucial lemma:

Lemma 4.1.2. *If* $\mathrm{char}(k) > 2$ *then*

$$H^2(V_a, k) = \Lambda^2 H^1(V, k) \oplus \bar{\omega} H^1(V_a, k).$$

The isomorphism between $H^1(V_a, k)$ and $\mathrm{Hom}(V_a, \mathbf{G}_a)$ allows us to use this theorem to *uniquely* identify groups by particular factor systems: an alternating factor system plus a factor system of *Witt type*. The following corollary is immensely important and will be used frequently and without remark for the remainder of the thesis.

Corollary 4.1.3. *Let* $\{f_i\}_{i \in I}$ *and* $\{g_i\}_{i \in I}$ *be a set of functions in* $\mathrm{Hom}(\mathbf{G}_a, \mathbf{G}_a)$ *indexed by the same indexing set* I *and let* ϕ *be another function in* $\mathrm{Hom}(\mathbf{G}_a, \mathbf{G}_a)$. *Every extension of* $\mathbf{G}_a$ *by* $\mathbf{G}_a$ *can be defined by a unique factor system* $\beta + \omega$ *where*

$$\beta(x, y) = \sum_{i \in I} f_i(x) g_i(y) - f_i(y) g_i(x)$$

and

$$\omega(x, y) = \frac{\phi(x)^p + \phi(y)^p - (\phi(x) + \phi(y))^p}{p}.$$

For a factor system $\beta + \omega$ *we call the associated extension* $\mathbf{H}_{\beta+\omega}$. *When* $\mathbf{H}_{\beta+\omega}$ *is defined over a finite field* $\mathbf{F}_q$, *we call* $\mathbf{H}_{\beta+\omega}(\mathbf{F}_q) = H_{\beta+\omega}$.

4.1.1 The Orbit Method

We recollect information on Lazard's exponential and the orbit method from [BD06]. Lazard's exponential gives us a particular equivalence of categories between nilpotent algebraic groups and nilpotent lie algebras when the nilpotence class is less than the characteristic. This is a substantial limitation, but does not restrict us for central extensions of $\mathbf{G}_a$ by $\mathbf{G}_a$ for odd primes.

Fix $c \geq 0$ a natural number. Let Nilp_c be the category of nilpotent groups of nilpotence class $\leq c$ with invertible map $g \to g^j$ for all $j \leq c$. Let $\mathfrak{nilp}_c$ be the category of nilpotent Lie algebras over $\mathbf{Z}[\frac{1}{c}]$ of nilpotence class $\leq c$.

Theorem 4.1.4 (M. Lazard)**.** *Given a Lie algebra* $\mathfrak{g}$ *which is nilpotent of class* $\leq c$ *one associates the nilpotent group* $\mathrm{Exp}(\mathfrak{g})$ *whose underlying set is the same as* $\mathfrak{g}$ *and whose multiplication is given by the Campbell-Baker-Hausdorff series*

$$x * y = \sum_{i \leq c} CH_i(x, y), \quad x, y \in \mathfrak{g}.$$

This assignment is functorial, and it determines an equivalence of categories $\mathfrak{nilp}_c \to \mathrm{Nilp}_c$*.*

As a warning, the Lie algebra $\mathrm{Lie}(G)$ is always a p-Lie algebra over the field k, while $\mathrm{Log}(G)$ need not be a k-vector space; in general it is only a Lie algebra over the ring $\mathbf{Z}[1/c!]$. The Lie bracket in $\mathrm{Log}(G)$ more closely reflects the group operation in G than the bracket in $\mathrm{Lie}(G)$. The equivalence from the theorem also furnishes maps $\log : G \to \mathrm{Log}(G)$ and $\exp : \mathrm{Log}(G) \to G$ which are the identity maps on the underlying sets, even though one might expect the ordinary exponential for exp. We provide details on the structure of $\mathrm{Log}(G)$ in Section 4.2.1.

Theorem 4.1.5. *[BD06] Let* Γ *be a finite group of nilpotence class* $\leq c$ *such that all the prime divisors of the order* $|\Gamma|$ *are greater than* c*. Let* $\mathfrak{g}$ *be* $\mathrm{Log}(\Gamma)$ *and let* $\mathfrak{g}^* = \mathrm{Hom}(\mathfrak{g}, \mathbf{C}^\times)$*, the set of abelian group homomorphisms from* $\mathfrak{g}$ *to* $\mathbf{C}^\times$*. Then* Γ *acts on* $\mathfrak{g}^*$ *by the coadjoint action and for every* Γ*-orbit* $\Omega \subset \mathfrak{g}^*$ *there exists an irreducible representation of* Γ *whose character is given by the formula*

$$\rho_\Omega(g) = \frac{1}{(\mathrm{card}\ \Omega)^{1/2}} \sum_{f \in \Omega} f(\log\ g) \qquad \forall g \in \Gamma.$$

This gives a bijection between Γ*-orbits in* $\mathfrak{g}^*$ *and irreducible representations of* Γ*.*

In particular, for an extension of $\mathbf{G}_a$ by $\mathbf{G}_a$ the nilpotence class is not more than 2, so if $\mathrm{char}(k) > 2$ then Lazard's exponential and the orbit method may be applied.

4.2 Calculating Characters

We use the orbit method to calculate the representations of $H = \mathbf{H}(\mathbf{F}_q)$ where $\mathbf{H}$ is a two dimensional unipotent group over an algebraically closed field k which is defined over $\mathbf{F}_q$. In order to use the orbit method, it is helpful to have first have an explicit presentation of $\mathfrak{h} = \mathrm{Log}(H)$: a non-canonical H-module isomorphism from $\mathfrak{h} \to \mathrm{Log}(H)$.

Once we have such an isomorphism, finding characters of $\mathfrak{h}$ is the same as understanding $\mathfrak{h}^* = \mathrm{Hom}(\mathfrak{h}, K^\times)$ where K is an algebraically closed field of characteristic 0. Those characters play an out-sized role in finding the characters of H.

4.2.1 The characters of $\mathfrak{h}$

Let $H = \mathbf{H}_{\beta+\omega}(\mathbf{F}_q)$ and let Log be the functor from $\mathrm{Nilp}_c \to \mathfrak{nilp}_c$ given by Lazard's exponential. The nilpotent lie algebra $\mathrm{Log}(H)$ has an abelian group structure related to Witt vectors as follows:

Proposition 4.2.1. *Suppose that H is the $\mathbf{F}_q$ points of an extension of $\mathbf{G}_a$ by $\mathbf{G}_a$ determined by the cocycle $\beta + \omega$ defined over $\mathbf{F}_q$. Then $\mathrm{Log}(H_{\beta+\omega}) \cong H_\omega$ as an additive group.*

Proof. Let the nilpotent algebraic group $H = H_{\beta+\omega}$ be the extension of $\mathbf{G}_a$ by $\mathbf{G}_a$ corresponding to the factor system $\beta + \omega$ and let $\mathfrak{h} = \mathrm{Log}(H)$. We begin with $a = (a_1, a_2), b = (b_1, b_2) \in H$. The proof strategy is to compare the product of $a *_H b$ as defined by factor systems with the product of $\log(a) *_{\mathrm{CBH}} \log(b)$ to give information about the bracket.

Using that $a^{-1} = (-a_1, -a_2)$ with the $*_H$ structure and that under $*_{\mathrm{CBH}}$ we have $\log(a)^{-1} = -\log(a)$ we can compute the commutator of a and b to see that

$$(0, 2\beta(a_1, b_1)) = [a, b].$$

Then, we calculate

$$\begin{aligned} a *_H b *_H (0, -\beta(a_1, b_1)) &= (a_1 + b_1, a_2 + b_2 + \omega(a_1, b_1)) \\ &= \log(a) +_{\mathfrak{h}} \log(b) +_{\mathfrak{h}} \frac{[\log(a), \log(b)]}{2} -_{\mathfrak{h}} \frac{[\log(a), \log(b)]}{2} \\ &= \log(a) +_{\mathfrak{h}} \log(b) \end{aligned}$$

which concludes the proof. □

Phrased differently, the bracket in $\mathfrak{h}$ corresponds exactly to the factor system β. This should not come as a surprise, since the group operation given by Lazard's exponential necessarily could not contain the data of a symmetric factor system.

Since $\mathrm{Log}(H) = \mathfrak{h}$ is isomorphic as an additive group to H_ω we can identify the dual $\mathfrak{h}^*$ by finding a perfect pairing $F : H_\omega \times H_\omega \to K^\times$: a group homomorphism which is non-degenerate and biadditive. That will allow us to identify $\mathfrak{h}$ with $\mathfrak{h}^*$.

Lemma 4.2.2. *Every extension H_ω of $\mathbf{G}_a$ by $\mathbf{G}_a$ can be embedded as a closed subgroup of $W_2 \times \mathbf{G}_a$.*

Proof. This is a specific case of the theorem from Serre as restated in Theorem 3.1.5 which states that every connected commutative unipotent group over a perfect field can be embedded in a product of truncated Witt vectors. We will write H_ω additively, as it is a commutative algebraic group.

Suppose that

$$\omega(x, y) = \frac{\phi(x)^p + \phi(y)^p - (\phi(x) + \phi(y))^p}{p}$$

where $\phi \in \mathrm{Hom}(\mathbf{G}_a, \mathbf{G}_a)$. Then, the group operation in H_ω is given by

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2 + \omega(a_1, b_1)).$$

It is now easy to check that the mapping $i : H_\omega \to W_2 \times \mathbf{G}_a$

$$(a, b) \mapsto (\phi(a), b, a)$$

is an injective homomorphism. □

In order to handle an arbitrary two dimensional unipotent group H we need to choose an identification of $\mathrm{Log}(H) = \mathfrak{h}$ with $\mathrm{Hom}(\mathfrak{h}, K^\times) = \mathfrak{h}^*$ by choosing a bilinear homomorphism $F : \mathfrak{h} \times \mathfrak{h} \to K^\times$. Making such a choice determines an explicit map $\mathfrak{h} \to \mathfrak{h}^*$ by

$$x \mapsto F(-, x)$$

and determines the representations of H_ω.

Now, suppose that $i : H_\omega \to W_2 \times \mathbf{G}_a$ is as above $\alpha_1 : \mathbf{F}_p \to K^\times$ and $\alpha_2 : \mathbf{Z}/p^2\mathbf{Z} \to K^\times$ are choices of a p-th and p^2 root of unity. That is, let $\alpha_1(1) = \zeta_p$ a p-th root of unity in K and $\alpha_2(1 + 0p) = \zeta_{p^2}$ a primitive p^2 root of unity. Let (a, b) and (c, d) be elements of H_ω. We say that a map $\psi \in \mathrm{Hom}(W_2 \times \mathbf{G}_a, K^\times)$ is non-degenerate if $\psi(g) \neq 1$ for all $g \in H_\omega$. The map ϕ which defines ω will determine a pairing.

Lemma 4.2.3. *Suppose ϕ induces an isomorphism of finite groups*

$$\phi : \mathbf{G}_a(\mathbf{F}_q) \to \mathbf{G}_a(\mathbf{F}_q).$$

Then $i : H_\omega(\mathbf{F}_q) \to W_2(\mathbf{F}_q)$ is an isomorphism of finite groups and

$$\psi_x(g) = \alpha_2 \operatorname{tr}(\phi(x_1)\phi(g_1), \phi(x_1)^p g_2 + \phi(g_1)^p x_2).$$

Proof. Once we show that i is an isomorphism the second statement follows since ψ_x is a character of W_2. Therefore we check that $\phi : \mathbf{G}_a(\mathbf{F}_q) \to \mathbf{G}_a(\mathbf{F}_q)$ induces an isomorphism $\phi' : H_\omega(\mathbf{F}_q) \to W_2(\mathbf{F}_q)$ by

$$\phi'(x_1, x_2) = (\phi(x_1), x_2).$$

Indeed, this is a homomorphism: we compute that

$$\phi'((x, 0) + (y, 0)) = \phi'(x + y, \omega(x, y))$$

is equal to

$$(\phi(x),0)+(\phi(y),0)=(\phi(x)+\phi(y),\omega'(\phi(x),\phi(y))$$

where ω' is the ordinary Witt factor system. The map ϕ' is injective because ϕ is injective. □

Lemma 4.2.4. *Suppose that ϕ does not induce an isomorphism of finite groups*

$$\phi:\mathbf{G}_a(\mathbf{F}_q)\to\mathbf{G}_a(\mathbf{F}_q)$$

and is nonzero. Then

$$\psi_{(\phi(c),d,c)}(\phi(a),b,a)=\alpha_2\operatorname{tr}(\phi(a)\phi(c),\phi(a)^pd+\phi(c)^pd)\alpha_1(\operatorname{tr}ac)$$

has $\psi_{i(x)}$ an element of $\operatorname{Hom}((W_2\times\mathbf{G}_a)(\mathbf{F}_q),K^\times)$, non-degenerate over $(\phi(a),b,a)$ for $(\phi(c),d,c)\neq(0,0,0)$ and ψ_x is not isomorphic to ψ_y for different elements $x=(\phi(x_1),x_2,x_1)$ and $y=(\phi(y_1),y_2,y_1)$.

Proof. This is a homomorphism by construction, Witt multiplication distributes across Witt addition. First we check non-degeneracy. Consider $\psi_x(g)$ over all $g=(\phi(g_1),g_2,g_1)\in(W_2\times\mathbf{G}_a)(\mathbf{F}_q)$. We have that

$$\psi_x(g)=\alpha_2\operatorname{tr}(\phi(x_1)\phi(g_1),\phi(x_1)^pg_2+\phi(g_1)^px_2)\alpha_1(\operatorname{tr}x_1g_1).$$

We can see that $\phi(x_1)$ must be equal to 0 since the first component is the only part that relates to a p^2 root of unity, so

$$\psi_x=\alpha_2\operatorname{tr}(0,\phi(g_1)^px_2)\alpha_1(\operatorname{tr}x_1g_1).$$

Because ϕ is not an isomorphism, there exists $g_1\neq0$ so that $\phi(g_1)=0$. Thus, if $\psi_x(g)=1$ for all g, then x_1 must be equal to 0. Thus,

$$\psi_x=\alpha_2\operatorname{tr}(0,\phi(g_1)^px_2)=1$$

implies that $x_2 = 0$ as well.

These are pairwise non-isomorphic as distinct characters of $(W_2 \times \mathbf{G}_a)(\mathbf{F}_q)$, so the argument is the same as it would be there: we can calculate

$$\langle \psi_x, \psi_y \rangle_{H_\omega} = \frac{1}{|H_\omega|} \sum_{g \in H_\omega} \psi_{x-y}(g),$$

which is the sum over all group elements of a nontrivial character, which is 0 whenever $x \neq y$. □

Theorem 4.2.5. *Suppose that $i : H_\omega \to W_2 \times \mathbf{G}_a$ has image $U = \{(\phi(x_1), x_2, x_1)\}$. A complete set of characters $\mathrm{Hom}(H_\omega(\mathbf{F}_q), \mathbf{C}^\times)$ can be given by the set of all ψ_x with $x \in H_\omega(\mathbf{F}_q)$ as follows:*

1. *If $\omega = 0$, define $\psi_x(y) = \alpha_1 \operatorname{tr}(x_1 y_1 + x_2 y_2)$.*
2. *If ϕ is an isomorphism of finite groups, define ψ_x as in Lemma 4.2.3*
3. *If $\omega \neq 0$ and ϕ not a finite group isomorphism, define ψ_x as in Lemma 4.2.4*

Proof. We need only check that the examples given are non-degenerate over the subset $i(H_\omega) \subset W_2 \times \mathbf{G}_a$ and pairwise non-isomorphic, since there are sufficiently many characters in each case to represent the class functions of an abelian group. The first is well known as a perfect pairing on $\mathbf{G}_a \times \mathbf{G}_a$, which is H_ω when $\omega = 0$. The second and third cases have those properties by Lemmas 4.2.3 and 4.2.4. □

Phrased in a different way, when $\omega = 0$, the "usual" dot product provides a non-degenerate pairing on $\mathbf{G}_a \times \mathbf{G}_a$ and so provides an identification of $\mathfrak{h}$ with $\mathfrak{h}^*$. Cases 2 and 3 are the pairings determined by Witt multiplication in $W_2 \times \mathbf{G}_a$.

As an abelian group, each element of the dual space provides a non-isomorphic character $\chi : H_\omega \to \mathbf{C}^\times$, so every element of $\mathfrak{h}^*$ can be given by $(x_1, x_2) = \psi_{(x_1, x_2)}$ in Theorem 4.2.5.

The Witt type data of a representation of $G = H_{\beta+\omega}$ is contained entirely in this choice. Since ω is symmetric, the formula for the adjoint action does not contain ω. It is also worth noting that alternating type data only alters the coadjoint orbit, since it necessarily could not be seen by the identification of $\mathfrak{h}^*$ and H_ω which gives $f \in \mathfrak{h}^*$.

4.2.2 Calculation of the coadjoint orbit

Theorem 4.2.1. *Let $\mathbf{F}_q$ be a finite field of order p^r and let $\mathbf{H}$ be an extension of $\mathbf{G}_a$ by $\mathbf{G}_a$ corresponding to the factor system $\beta+\omega$ and $H = \mathbf{H}(\mathbf{F}_q)$. Let $\alpha_1 : \mathbf{Z}/p\mathbf{Z} \to K^\times$ and $\alpha_2 : \mathbf{Z}/p^2\mathbf{Z} \to K^\times$ be choices for a primitive p-th and p^2 root of unity and let* $\mathrm{tr} = \mathrm{tr}_{\mathbf{F}_q/\mathbf{F}_p}$.

1. *If $\omega = 0$, then elements of the coadjoint orbit of $\psi_{(u,w)}$ are of the form $\psi_{(u',w)}$ and the characters of irreducible representations are given by*

$$\rho_\Omega(g_1, g_2) = \frac{1}{(\text{card }\ \Omega)^{1/2}} \sum_{(u,w)\in\Omega} \alpha_1 \,\mathrm{tr}(ug_1 + wg_2) \qquad \forall (g_1, g_2) \in H.$$

2. *If $\omega \neq 0$ then*

$$\omega(x, y) = \frac{\phi(x)^p + \phi(y)^p - (\phi(x) + \phi(y))^p}{p}.$$

Elements of the coadjoint orbit of $\psi_{(u,w)}$ are of the form $\psi_{(u,w')}$ and the characters of irreducible representations are given by $\rho_\Omega(g_1, g_2)$ which equals

$$\frac{1}{M} \sum_{(u,w)\in\Omega} \alpha_2 \,\mathrm{tr}(\phi(u)\phi(g_1), \phi(u)^p g_2 + \phi(g_1)^p w) \cdot \alpha_1(\mathrm{tr}\, g_1 u)$$

when ϕ is not an isomorphism and

$$\frac{1}{M} \sum_{(u,w)\in\Omega} \alpha_2 \,\mathrm{tr}(\phi(u)\phi(g_1), \phi(u)^p g_2 + \phi(g_1)^p w)$$

if ϕ is an isomorphism for every $(g_1, g_2) \in H_\omega$ and $M = (\text{card }\ \Omega)^{1/2}$.

Proof. In order to calculate the coadjoint action we first need to calculate the adjoint action. Let H be an arbitrary extension of $\mathbf{G}_a$ by $\mathbf{G}_a$ and $\mathrm{Log}(H) = \mathfrak{h}$ with $(g_1, g_2) \in H$ and $(v_1, v_2) \in \mathfrak{h}$. We can conjugate (v_1, v_2) by (g_1, g_2) to get

$$(g_1, g_2)(v_1, v_2)(-g_1, -g_2) = (g_1 + v_1, g_2 + v_2 + \beta(g_1, v_1) + \omega(g_1, v_1))(-g_1, -v_1)$$

which is equal to

$$(v_1, v_2 + \beta(g_1, v_1) + \omega(g_1, v_1) + \beta(g_1 + v_1, -g_1) + \omega(g_1 + v_1, -g_1)).$$

Now, because ω is a factor system

$$\omega(g_1 + v_1, -g_1) + \omega(g_1, v_1) = \omega(g_1, -g_1) + \omega(g_1 - g_1, v_1) = 0,$$

and since β is biadditive and alternating we can conclude

$$(g_1, g_1)(v_1, v_2)(-g_1, -g_2) = (v_1, v_2 + 2\beta(g_1, v_1)).$$

This gives a coadjoint action on $\mathfrak{g}^*$ that only depends on β and our choice of pairing from Theorem 4.2.5. This action is a map $G \times \mathfrak{g}^* \to \mathfrak{g}^*$ which is not in general a morphism of varieties.

Given a pairing $(u, w) \to \psi_{(u,w)} \in \mathfrak{g}^*$ and $(v_1, v_2) \in \mathfrak{g}$, an element (u', w') is in the $H_{\beta+\omega}$ orbit of (u, w) only if

$$\psi_{(u',w')}(v_1, v_2) = \psi_{(u,w)}(v_1, v_2 + 2\beta(g_1, v_1))$$

for some $g_1 \in \mathbf{G}_a$. Since that action depends on which perfect pairing we use, we divide now into three cases.

1. When ω is 0, we solve for u' and w' when

   $$\psi_{(u',w')}(v_1, v_2) = \alpha_1(\mathrm{tr}_{\mathbf{F}_q/\mathbf{F}_p}(uv_1 + w(v_2 + 2\beta(g_1, v_1))).$$

   This gives that $w' = w$ because the coefficient of v_2 is w' on the left and w on the right. The coefficient of v_1 is dependent on β, so $u' = u + f(g_1, w)$ with f a polynomial in p-th powers and roots of g_1 and w.

2. When ϕ is an isomorphism solving for u' and w' in

$$\psi_{(u',w')} = \alpha_2 \operatorname{tr}(\phi(u)\phi(v_1), \phi(u)^p(v_2 + 2\beta(g_1, v_1)) + \phi(v_1)^p w)$$

has that $\phi(u') = \phi(u)$ as the only coefficient of v_2. Then, $w' = w + f(v_1, u)$ for a polynomial in p-th powers and roots of g_1 and u.

3. When ϕ is not an isomorphism and nontrivial we need to use the third pairing from Theorem 4.2.5. This gives that $\psi_{(u',w')}$ is equal to

$$\alpha_2 \operatorname{tr}(\phi(u)\phi(v_1), \phi(u)^p(v_1 + 2\beta(g_1, v_1)) + \phi(v_1)^p w)\alpha_1(\operatorname{tr} ac).$$

Similar to (2), this gives $u' = u$ and forces that $w' = w + f(v_1, u)$ for an appropriate polynomial $f(v_1, u)$.

□

4.3 Examples

Suppose that k is an algebraically closed field of characteristic p, $q = p^r$, $\beta(x, y) = x^p y - xy^p$ and $\omega(x, y) = \frac{x^p + y^p - (x+y)^p}{p}$. We calculate the representations of $H_\beta(\mathbf{F}_q)$, $H_\omega(\mathbf{F}_q)$ and $H_{\beta+\omega}(\mathbf{F}_q)$ in certain cases and compare. For ease of notation, let $\operatorname{tr} = \operatorname{tr}_{\mathbf{F}_q/\mathbf{F}_p}$. Notice that both factor systems are defined for all $\mathbf{F}_q$ and that β is a trivial factor system unless $r \geq 2$.

Example 4.3.1. For H_β, since $\omega = 0$, we use the dot product. The computation of the coadjoint orbit gives that (u', v') is in the orbit if

$$\begin{aligned}(u', w')(v_1, v_2) &= \alpha(\operatorname{tr}(uv_1 + w(v_2 + \beta(g_1, v_1)))) \\ &= \alpha(\operatorname{tr}(uv_1 + wv_2 + wg_1^p v_1 - wg_1 v_1^p))\end{aligned}$$

for some $g_1 \in \mathbf{G}_a$. We can isolate v_1 by taking p-th roots, so

$$(u', w') = (u + wg_1^p - w^{1/p} g_1^{1/p}, w).$$

Notice that the size of the coadjoint orbits (and hence the dimension of the representation) is dependent on both the factor system and the field in which we are working. Suppose $p = 3$ and $r = 2$. Then the sizes of the representations are given by

Element of $\mathfrak{g}^*$	coadjoint orbit size
(u, w_p) for every $w_p \in \mathbf{F}_3$ and every $u \in \mathbf{F}_9$	1
$(0, w)$ for $w \notin \mathbf{F}_3$	9.

Compare this to the result when $r = 3$

Element of $\mathfrak{g}^*$	coadjoint orbit size
$(0, 0)$	1
(u, w) for every $u, w \in \mathbf{F}_{27}$ with $(u, w) \neq (0, 0)$	9.

The difference between the two situations is the existence of every element of $\mathbf{F}_9$ when $r = 2$ but not when $r = 3$.

Now, consider $\mathbf{F}_q = \mathbf{F}_{p^2}$. Since the coadjoint orbit of an element $(u, w) \in \mathfrak{g}^*$ is given by

$$(g_1, g_2) \cdot (u, w) = (u + w g_1^p - w^{1/p} g_1^{1/p}, w)$$

we consider

$$w g_1^p - w^{1/p} g_1^{1/p}. \tag{4.1}$$

Now, there are two cases, those where $w \in \mathbf{F}_p$ and those where $w \notin \mathbf{F}_p$. If $w \in \mathbf{F}_p$, then (4.1) is equal to

$$w(g_1^p - g_1^{1/p})$$

which is 0 whenever $g_1^{p^2} = g_1$, which is true for every element of $\mathbf{F}_{p^2}$. Therefore the coadjoint orbit has a single element whenever $w \in \mathbf{F}_p$. There are $p^2 \cdot p$ elements of H_β with $u \in \mathbf{F}_{p^2}$ and $w \in \mathbf{F}_p$.

Now, suppose that $w \notin \mathbf{F}_p$. This means that $w^{1/p} \neq w$, otherwise w would be in $\mathbf{F}_p$. Then, since $g_1^{1/p} = g_1^p$ for all elements of $\mathbf{F}_{p^2}$,

$$g_1(w^{1/p} - w) \neq 0$$

for $g_1 \neq 0$. Thus the orbit has p^2 elements. This gives $p^2 - p$ elements v_2 which have orbit size p^2. This accounts for every element of the coadjoint orbit, so it gives every representation of H_β.

Example 4.3.2. Now we consider the representations of H_ω. Notice that $H_\omega = W_2$, the length 2 Witt vectors which is an abelian group. Indeed, the coadjoint action is trivial so each coadjoint orbit has a single element. Therefore, each representation is given by an element of W_2 and a fixed map $\alpha_2 : \mathbf{Z}/p^2\mathbf{Z} \to K^\times$. Given an element $(a,b) \in H_\omega$, since ϕ is the identity map our pairing gives

$$\rho_{(a,b)}(g_1, g_2) = \alpha\,\mathrm{tr}(ag_1, a^p g_2 + g_1^p b)$$

which are exactly the characters of W_2.

Example 4.3.3. We can compare the previous examples to $H_{\beta+\omega}$. We begin again by calculating the coadjoint orbit

$$\begin{aligned}(u', w')(v_1, v_2) &= \alpha\,\mathrm{tr}(uv_1, u^p(v_2 + \beta(g_1, v_1)) + v_1^p w)\\ &= \alpha\,\mathrm{tr}(uv_1, u^p(v_2 + g_1^p v_1 - g_1 v_1^p) + v_1^p w)\\ &= \alpha\,\mathrm{tr}(uv_1, u^p v_2 + v_1^p(g_1^{p^2} u^{p^2} - g_1 u^p + w))\end{aligned}$$

which implies that

$$(u', w') = (u, w + u^{p^2} g_1^{p^2} - u^p g_1).$$

A point is stabilized if $u^{p^2} g_1^{p^2} = u^p g_1$, which is the same kind of $\mathbf{F}_{p^2}$ behavior that we had in Example 4.3.1 (it is the p-th power of Equation 4.1). In particular if $p = 3$ and $r = 2$ the sizes of the representations are given by

Element of $\mathfrak{g}^*$	coadjoint orbit size
(u_p, w) for every $u_p \in \mathbf{F}_3$ and every $w \in \mathbf{F}_9$	1
$(u, 0)$ for $u \notin \mathbf{F}_3$	9.

even though the representations themselves are necessarily different because of the existence of elements of order p^2.

4.4 Linear Embedding

We embed the extension of $\mathbf{G}_a$ by $\mathbf{G}_a$ when $\mathrm{char}(k) > 2$ into a sufficiently large subgroup of GL_n. In particular, fake Heisenberg groups, the groups corresponding to alternating factor systems, embed into extended Heisenberg groups.

Because of the sizes of the involved matrices, we first show the alternating case and then the Witt case. The methodology for $H_{\beta+\omega}$ follows immediately.

Remark 4.4.1. For two dimensional unipotent groups, we can find an embedding as follows: let $k[S,T]$ be the group ring from H where $S(s,t) = s$ and $T(s,t) = t$. Let H act on $k[S,T]$ by the left regular action. For any given group structure of H, we can find a finite dimensional vector subspace V of $k[S,T]$ which is stable under that action. The data of that action gives a subgroup of $GL(V)$ which is isomorphic to H.

4.4.1 Linear Embedding of H_β

Theorem 4.4.2. *Suppose that* $|I| = m$ *and*

$$\beta(x,y) = \sum_{i\in I} f_i(x)g_i(y) - f_i(y)g_i(x).$$

Then, the extension of $\mathbf{G}_a$ *by* $\mathbf{G}_a$ *defined by* β *is isomorphic as an extension to a subgroup of* GL_{m+3} *over* k*. In particular, it is a subgroup of the ordinary Heisenberg group of dimension* $2m+3$*.*

Proof. First, we construct a subset that contains both the data of $\mathbf{G}_a$ and of β. We will then check that it is a group, and that it is isomorphic to the group defined by the extension $\beta^+(x,y) = \sum_{i\in I} f_i(x)g_i(y)$. Finally, we will check that the extension defined by β^+ only differs by a trivial extension by the one defined by β.

Let $M(v,t)$ be the matrix

$$M(v,t) = \begin{pmatrix} 1 & v & f_1(v) & f_2(v) & \cdots & f_m(v) & t \\ 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 & g_1(v) \\ 0 & 0 & 0 & 1 & \cdots & 0 & g_2(v) \\ \vdots & & \vdots & & \vdots & & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & g_m(v) \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Now, let S be the set of elements

$$S = \{M(v,t) | v \in V, t \in k\}.$$

Then, because f and g are additive functions, S is a group. The map

$$M(v,t) \mapsto (v,t)$$

is a surjection to $\mathbf{G}_a \times \mathbf{G}_a$ and the kernel is only the identity matrix. Furthermore,

$$M(v,t_1)M(w,t_2) = M(v+w, t_1 + t_2 + \beta^+(v,w))$$

by construction. This gives us that our naive map is in fact a morphism onto the group defined by the factor system β^+.

Finally, to show that β^+ only differs from β by a trivial factor system, it's sufficient to find such a factor system. The map

$$p(x) = \beta^+(x,x)/2 : V \to k$$

has

$$\partial p(x,y) = \frac{1}{2}\beta^+(x,x) + \beta^+(y,y) - \beta^+(x+y,x+y))$$

which is equal to

$$\partial p(x,y) = -\frac{1}{2}(\beta^+(x,y) + \beta^+(y,x)).$$

Therefore

$$\beta^+ + \partial p = \frac{\beta(x,y)}{2}.$$

□

It is important to note that this map is not necessarily minimal or unique.

Example 4.4.3. The theorem says that the group H_β given by $\beta(x,y) = x^p y - x y^p$ can be put into a matrix group as

$$\begin{pmatrix} 1 & x & x^p & t \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & x \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

or as

$$\begin{pmatrix} 1 & x & x^p & -x & t \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & x \\ 0 & 0 & 0 & 1 & x^p \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

However, the minimal embedding is

$$\begin{pmatrix} 1 & x & t \\ 0 & 1 & x^p \\ 0 & 0 & 1 \end{pmatrix}.$$

4.4.2 Linear Embedding of H_ω

In a very similar way we can embed arbitrary factor systems of Witt type into matrix groups. We begin with an example

Example 4.4.4. Let $\mathrm{char}(k) = 3$ and

$$\omega(x,y) = \frac{(x+y)^3 - x^3 - y^3}{3} = x^2y + xy^2.$$

Then we can send an arbitrary $(v,t) \in H_\omega$ to the matrix

$$M(v,t) = \begin{pmatrix} 1 & v & v^2 & t \\ 0 & 1 & 2v & v^2 \\ 0 & 0 & 1 & v \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

We can calculate

$$M(v_1,t_1)M(v_2,t_2) = \begin{pmatrix} 1 & v_1+v_2 & v_1^2+2v_1v_2+v_2^2 & t_1+t_2+v_1^2v_2+v_1v_2^2 \\ 0 & 1 & 2v_1+2v_2 & v_1^2+2v_1v_2+v_2^2 \\ 0 & 0 & 1 & v_1+v_2 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

which is

$$M(v_1+v_2, t_1+t_2+\omega(v_1,v_2)) = \begin{pmatrix} 1 & v_1+v_2 & (v_1+v_2)^2 & t_1+t_2+\omega(v_1,v_2) \\ 0 & 1 & 2v_1+2v_2 & (v_1+v_2)^2 \\ 0 & 0 & 1 & v_1+v_2 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

This generalizes to the following lemma.

Lemma 4.4.5. *Let $p > 2$, $\phi \in \mathrm{Hom}(\mathbf{G}_a, \mathbf{G}_a)$ and*

$$\omega(x,y) = \frac{(\phi(x)+\phi(y))^p - \phi(x)^p - \phi(y)^p}{p}.$$

Then $H_\omega(\mathbf{F}_q)$ can be embedded into $\mathrm{GL}_{p+2}(\mathbf{F}_q)$.

Proof. Let $(v,t) \in H_\omega$. Define

$$M(v,t) = \begin{pmatrix} 1 & v & \phi(v) & \phi(v)^2 & \cdots & \phi(v)^{p-1} & t \\ 0 & 1 & 0 & 0 & & 0 & 0 \\ 0 & 0 & 1 & \binom{2}{1}\phi(v) & \cdots & \binom{p-1}{1}\phi(v)^{p-2} & \binom{p}{1}\phi(v)^{p-1} \\ 0 & 0 & 0 & 1 & & \binom{p-1}{2}\phi(v)^{p-3} & \binom{p}{2}\phi(v)^{p-2} \\ \vdots & & & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \binom{p-1}{p-2}\phi(v) & \binom{p}{p-2}\phi(v)^2 \\ 0 & 0 & 0 & 0 & & 1 & \binom{p}{p-1}\phi(v) \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Then, $M(v_1,t_1)M(v_2,t_2)$ is equal to $M(v_1+v_2, t_1+t_2+\omega(v_1,v_2))$ by construction which gives a bijection from H_ω onto the set $S = \{M(v,t) | v,t \in \mathbf{F}_q\}$. □

Theorem 4.4.6. *Suppose that* $|I| = m$

$$\beta(x,y) = \sum_{i \in I} f_i(x)g_i(y) - f_i(y)g_i(x)$$

and

$$\omega(x,y) = \frac{(\phi(x)+\phi(y))^p - \phi(x)^p - \phi(y)^p}{p}$$

for f_i, g_i *and* ϕ *in* $\mathrm{Hom}(\mathbf{G}_a, \mathbf{G}_a)$. *Then, every factor system* $\beta + \omega$ *can be embedded in* GL_{m+p+2}.

Proof. This follows immediately from the construction in Lemma 4.4.1 and Lemma 4.4.2. □

$$
\begin{pmatrix}
1 & v & f_1(v) & \cdots & f_m(v) & \phi(v) & \phi(v)^2 & \cdots & \phi(v)^{p-1} & t \\
0 & 1 & 0 & & 0 & 0 & 0 & & 0 & 0 \\
0 & 0 & 1 & \cdots & 0 & 0 & 0 & \cdots & 0 & g_1(v) \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 1 & 0 & 0 & \cdots & 0 & g_m(v) \\
0 & 0 & 0 & & 0 & 1 & \binom{2}{1}\phi(v) & \cdots & \binom{p-1}{1}\phi(v)^{p-2} & \binom{p}{1}\phi(v)^{p-1} \\
0 & 0 & 0 & \cdots & 0 & 0 & 1 & & \binom{p-1}{2}\phi(v)^{p-3} & \binom{p}{2}\phi(v)^{p-2} \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & \binom{p-1}{p-2}\phi(v) & \binom{p}{p-2}\phi(v)^2 \\
0 & 0 & 0 & & 0 & 0 & 0 & & 1 & \binom{p}{p-1}\phi(v) \\
0 & 0 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0 & 1
\end{pmatrix}
$$

Chapter 5

Representations of $U \rtimes T$

Suppose that U is a two dimensional unipotent group over an algebraically closed field k as in Chapter 4 and suppose T is a torus. Since k is algebraically closed, T is isomorphic to a product of multiplicative groups $T \cong \mathbf{G}_m^i$ for some positive integer i.

In the first section, we find necessary and sufficient conditions for a torus to act on U by automorphisms. If such an action exists for a torus T, we can build the group $G = U \rtimes T$ with the given automorphism.

In the second section, we use representation theoretic tools from [CR06] and [Ser77] to find irreducible representations of G. We indicate a procedure for describing all irreducible representations of G first over a sufficiently large field K of characteristic 0, and then over a field κ of characteristic $\ell \neq p$.

We the conclude the chapter by continuing Example 4.3.1 from the previous chapter by calculating the irreducible κ-representations of the group $H_\beta \rtimes T$ for the factor system $\beta(x,y) = x^p y - xy^p$.

5.1 Torus Actions

Let U be a two dimensional unipotent group over k an algebraically closed field characteristic > 2. A torus T acts by morphisms on U if the group action is defined by a morphism of algebraic varieties

$$T \times U \to U$$

given by $(a,u) \to a \cdot u$. Then, T acts by *group automorphisms* if for every $a \in T$ and $u, v \in U$

$$a \cdot uv = (a \cdot u)(a \cdot v).$$

Notice that a is necessarily an automorphism and not just an endomorphism since $a^{-1} \in T$.

As in [McN14], a group action of G on an algebraic group U is *linear* if there exists a G-equivariant isomorphism between U and $\mathrm{Lie}(U)$. Given a linear action, we can lift an action of G on $\mathrm{Lie}(U)$ to an action on U. By [McN14, Proposition 3.2.3] any action of G on a one dimensional vector group is linear. Since T acts on $\mathrm{Lie}(\mathbf{G}_a)$ by weights, it acts by weights on $\mathbf{G}_a$ as well. In particular, given a T action on $\mathbf{G}_a$ it must be of the form

$$t.x = \lambda(t)x$$

for some character λ.

The following example demonstrates the difficulty of extending an action by weights to an arbitrary two dimensional unipotent group:

Example 5.1.1. Suppose that T is a one dimensional torus, $\mathbf{G}_m$, which acts by automorphisms on a two dimensional unipotent group H defined by a factor system γ. Fix a polynomial $p \in k[T]$, the trivial factor system ∂p, and let H' be the extension defined by the factor system $\gamma + \partial p$.

Then, H and H' are isomorphic. There is an isomorphism $\phi : H \to H'$ which takes

$$\phi : (h_1, h_2) \mapsto (h_1, h_2 + p(h_1)).$$

If T acts on H by

$$a \cdot (h_1, h_2) = (\lambda(a)h_1, \mu(a)h_2)$$

then the isomorphism above determines an action of T on H' by

$$a \cdot (x_1, x_2) = (\lambda(a)x_1, \mu(a)x_2 + p(\lambda(a)x_1) - \mu(a)p(x_1))$$

for each $(x_1, x_2) \in H'$. Therefore, we should not expect that every torus action on an arbitrary H is given by weights on the factors.

This situation is more general than problems arising from trivial factor systems. If V is a vector space with a linear action of T then T is a direct sum of weight spaces. However, if M is any element of $\mathrm{GL}(V)$ then there is a new action of T on V according to the rule

$$a * v = (MaM^{-1})v.$$

If we write V' for V equipped with this action, then M determines an isomorphism between V and V'. While V' is still a direct sum of weight spaces, its weight spaces are not the same as those of V.

There are some situations in which we can always find a torus action. Suppose H is defined by the factor system γ. We say that γ is homogeneous of degree i if $\gamma(ax, ay) = a^i\gamma(x, y)$.

Proposition 5.1.2. *Suppose H is defined by a factor system $\gamma + \partial p$ where ∂p is a trivial factor system, and γ is of degree i. Then a one dimensional torus acts on H.*

Proof. To find the torus action on H, we find use the isomorphism to the group H' defined by γ. The action $a \cdot (x_1, x_2) = (a^j x_1, a^{ij} x_2)$ for $a \in T$ and $x_1, x_2 \in H'$ gives an action of T on H' by automorphisms because

$$a^j\gamma(a^i x_1, a^i x_2) = a^{ij}\gamma(x_1, x_2).$$

Then, the induced action on H is given by applying the isomorphism $\phi : H \to H'$, taking the T action on $\phi(H)$ and then taking the ϕ^{-1}. Given $(h_1, h_2) \in H$,

$$a \cdot (h_1, h_2) = (a^j h_1, a^{ij} h_2 - a^{ij} p(h_1) + p(a^j h_1)).$$

□

An arbitrary action on U is given by $a \cdot (x_1, x_2) = (a \cdot x_1, a \cdot x_2 + f(x_1, a))$ with $f(U,T) \in k[U,T,T^{-1}]$ and the actions on x_1 and x_2 given by potentially distinct weights. We can find conditions on f using the definition of a group action. Since

$$st(x_1, x_2) = ((st) \cdot x_1, (st) \cdot x_2 + s \cdot f(x_1, t) + f(t \cdot x_1, s))$$

and

$$st(x_1, x_2) = ((st) \cdot x_1, (st) \cdot x_2 + f(x_1, st)),$$

we have the equality

$$s \cdot f(x_1, t) + f(t \cdot x_1, s) = f(x_1, st). \tag{5.1}$$

Even for arbitrary double sum f in two variables, this condition is quite restrictive.

Lemma 5.1.3. *The only polynomials $f(X,Y)$ which satisfy (5.1) are $Y^b p(X) - p(Y^a X)$ for any k-polynomial p.*

Proof. Let $f(X,Y) = \sum_i \sum_j a_{ij} X^i Y^j$ where j is an integer and i is non-negative. Let the weight on the first variable be $t \cdot x_1 = t^a x_1$ and the weight in the second variable be $t \cdot x_2 = t^b x_2$ so that (5.1) gives

$$s^b f(x_1, t) + f(t^a x_1, s) - f(x_1, st) = 0.$$

Writing that as a double sum gives

$$\sum_i \sum_j a_{ij} x_1^i (s^b t^j + s^j t^{i+a} - s^j t^j) = 0$$

where a and b are fixed. Now we can find conditions on a_{ij} so that this becomes a sum in only one index i. Fix an i and suppose that $j \neq b$ and $j \neq i + a$. Then $s^b t^j + s^j t^{i+a} - s^j t^j$ has an $a_{ij} x^i s^b t^j$ which can not be canceled by the other two terms for any j other than the two listed. Therefore a_{ij} is 0 for any $j \neq b$ and $j \neq i+a$. For a fixed i, the remaining a_{ij} have the property that $a_{ib} = -a_{i(i+a)}$, which is independent of j. Therefore

$$F(X,Y) = \sum_i a_{ib} (X^i Y^b - X^i Y^{i+a}).$$

□

This leads to necessary and sufficient conditions for existence of a torus action on a two dimensional unipotent group.

Theorem 5.1.1. *Suppose $T = \mathbf{G}_m(\mathbf{F}_q)$ is a torus defined over $\mathbf{F}_q$ and that T acts (by $\mathbf{F}_q$-morphisms) on the group U by the rule $t\cdot(u_1,u_2) = (t^a u_1, t^b u_2 + t^b p(u_1) - p(t^a u_1))$. If U is defined by the factor system γ then $\gamma + \partial p$ is homogeneous for some polynomial $p \in k[T]$. If $\gamma + \partial p$ is homogeneous of degree i, then $b = ia$. Thus there exists a nontrivial torus action if and only if U is isomorphic to a group defined by a homogeneous factor system.*

Proof. Let U' be the group defined by the factor system $\gamma + \partial p$. The isomorphism between U and U' is given by $\phi : (u_1,u_2) \to (u_1, u_2 + p(u_1))$. If $(x_1,x_2) \in U'$,

$$t \cdot \phi^{-1}(x_1,x_2) = (t^a x_1, t^b x_2 + t^b p(x_1) - p(t^a x_1) - t^b p(x_1)).$$

Then,

$$\phi(t \cdot \phi^{-1}(x_1,x_2)) = (t^a x_1, t^b x_2).$$

Since this is an action on U' by automorphisms,

$$t \cdot (x_1 + y_1, x_2 + y_2 + \gamma(x_1,y_1) + \partial p(x_1,y_1)) = (t \cdot (x_1,x_2))(t \cdot (y_1,y_2))$$

it follows that

$$\gamma(t^a x_1, t^a y_1) + \partial(t^a x_1, t^a y_1) = t^b(\gamma(x_1,y_1) + \partial p(x_1,y_1)).$$

Therefore $\gamma + \partial p$ is homogeneous and if it is homogeneous of degree i then $b = ai$. □

5.2 Representations of G

Let k be an algebraically closed field of characteristic p and let $\mathbf{G}$ be an algebraic group defined over k. The group of points of G over a finite field $\mathbf{F}_q$, $\mathbf{G}(\mathbf{F}_q) = G$, form a finite group. We proceed as in [Ser77, Chapter 14]. Let K be a sufficiently large field with respect to $\mathbf{G}(\mathbf{F}_q)$ which is complete with respect to a discrete valuation v with valuation ring A, maximal ideal $\mathfrak{m}$ and residue field $\kappa = A/\mathfrak{m}$. Assume that $\mathrm{char}(K) = 0$ and $\mathrm{char}(\kappa) = \ell \neq p$. One in general can take κ to be $\mathbf{F}_{\ell^a}$ for some a

and let K be the unramified extension of $\mathbf{Q}_\ell$ with residue field κ. Let $\mathbf{U}$ be a two dimensional unipotent group over an algebraically closed field k of characteristic p and let $\mathbf{T}$ be a one dimensional algebraic torus $\mathbf{G}_m$ that acts on $\mathbf{U}$. We name the finite groups $U = \mathbf{U}(\mathbf{F}_q)$ and $T = \mathbf{T}(\mathbf{F}_q)$.

Now, let T act by $\mathbf{F}_q$ morphisms on U and define $G = U \rtimes T$. Then U is a normal subgroup of G. Our goal is to find the irreducible characters of G over a K then over κ. Since U is a p-group, representation theory of U is the same over both fields while the representations of G becomes more complicated over κ.

In both cases we will need Clifford theory as found in [CR06, Chapter 11] to give information about sub-characters of an irreducible character of G. We recall two useful theorems:

Theorem 5.2.1 (Clifford Theory)**.** *[CR06, Theorem 11.1] Let F be an arbitrary field, H a normal subgroup of a finite group G, M a simple FG-module, and L a simple FH-submodule of $\operatorname{res}^G_H(M)$. Then the following statements hold*

1. $\operatorname{res}^G_H(M)$ *is a semisimple FH-module, and is isomorphic to a direct sum of conjugates of L.*

2. *The FH-homogeneous components of* $\operatorname{res}^G_H(M)$ *are permuted transitively by G.*

3. *Let $\tilde{L}$ be the FH-homogeneous components of* $\operatorname{res}^G_H(M)$ *containing L, and let $\tilde{H} = \{x \in G : x\tilde{L} = L\}$, the stabilizer of $\tilde{L}$. Write G as a disjoint union $G = \bigcup_{i=1}^n g_i\tilde{H}$. Then $\{g_iL : 1 \leq i \leq n\}$ is a complete set of non-isomorphic conjugates of L, and each appears with the same multiplicity e in* $\operatorname{res}^G_H(M)$*:*

$$\operatorname{res}^G_H(M) \cong (\oplus_{i=1}^n {}^{g_i}L)^{(e)}\,.$$

4. *Let $\tilde{L}$ and $\tilde{H}$ be as in* (3)*. Then $\tilde{L}$ is a $F\tilde{H}$ module, and*

$$M = \operatorname{ind}^G_{\tilde{H}}(\tilde{L}).$$

The *FH-homogeneous components* in (2) are isomorphism classes of simple left

FH-submodules of $\mathrm{res}_H^G(M)$. These are sometimes called the "isotypic components".

Theorem 5.2.2. *[CR06, Theorem 11.5] Let $\psi \in \mathrm{Irr}_F(H)$ where $H \trianglelefteq G$, and let $S = G_\psi$, the stabilizer of ψ in G. Suppose that $\psi = \psi^1|_H$ for some F-character ψ^1 of S, that is, suppose that ψ can be extended to a character ψ^1 of S. Then*

1. $\psi^1 \in \mathrm{Irr}_F(S)$
2. *Each $\omega \in \mathrm{Irr}_F(S/H)$ can be viewed as an irreducible K-character of S, and we have $\mathrm{ind}_S^G(\omega\psi^1) \in \mathrm{Irr}_F(G)$ for each ω.*
3. *The formula $\mathrm{ind}_S^G \psi = \sum \omega(1) \,\mathrm{ind}_S^G(\omega\psi^1)$, where the sum extends over all $\omega \in \mathrm{Irr}_F(S/H)$, gives $\mathrm{ind}_H^G \psi$ as a linear combination of distinct irreducible characters $\mathrm{ind}_S^G(\omega\psi^1)$.*

Chapter 4 gives us complete information about the irreducible KU and κU-modules. Our goal is to lift a character of U to its stabilizer S using Theorem 5.2.2. Then, we will show that induction from an irreducible representation of S to G will be irreducible regardless of the field.

However, in order to use Theorem 5.2.2, we need to be able to *extend* an irreducible representation ρ of U to S: we would like to be able to say that for every irreducible representation (ρ, V) of U there exists an irreducible representation (ρ^1, V) of S.

The following lemma gives existence of such an extension for every irreducible representation of U:

Lemma 5.2.3. *Suppose that T is a cyclic group $T = \langle t \rangle$, $G = U \rtimes \langle t \rangle$, $(\psi, V) \in \mathrm{Irr}(U)$ and $V \cong^t V$. Then ψ is extendable to G.*

Proof. Given an irreducible representation ψ of U, the goal is to build an irreducible representation $\tilde{\psi}$ of V from ψ. The complication here is in building a homomorphism from the module isomorphism between V and ${}^tV$.

Fix a U isomorphism α with $\alpha \cdot V \to^t V$. Now, if $t^m = 1$, we can map which we will call α^m from $V \to^{t^m} V = V$. Thus α^m is a scalar which we will call $a \in k^\times$. Since

k is algebraically closed, we can choose $d \in k^\times$ with $d^m = a$. We re-define $\alpha = \frac{1}{d}\alpha$ so that $\alpha^m = \mathrm{id}$.

We can denote α by a matrix in $\mathrm{GL}(V)$ and α^i as the matrix product. Let $\tilde{\psi} : U \rtimes T \to \mathrm{GL}(V)$ be given by the map

$$(u, t^i) \mapsto \psi(u)\alpha^i.$$

The product of two elements in G is given by

$$(u, t^i)(u', t^j) = (u \cdot^{t^i} u', t^{i+j}).$$

To check that $\tilde{\psi}$ is a homomorphism, we apply it to both sides. We can compute

$$\tilde{\psi}(u, t^i)\tilde{\psi}(u', t^j) = \psi(u)\alpha^i\psi(u')\alpha^j$$

which is equal to

$$\psi(u)\left[{}^{t^i}\psi(u')\right]\alpha^{i+j}.$$

This is exactly equal to $\tilde{\psi}(u \cdot^{t^i} u', t^{i+j})$, so $\tilde{\psi}$ is a homomorphism. □

Let S be the stabilizer of an irreducible representation ρ_Ω of U. Then S/U is cyclic. It follows immediately that ρ_Ω is invariant in S. Thus, an irreducible character of U will always extend to its stabilizer.

Suppose that $\mathfrak{u} = \mathrm{Log}(\mathbf{U})$ and that $\rho_\Omega \in \mathrm{Irr}(\mathbf{U})$ is a character associated to the coadjoint orbit Ω in $\mathfrak{u}^* = \mathrm{Hom}(\mathfrak{u}, K)$ or $\mathfrak{u}^* = \mathrm{Hom}(\mathfrak{u}, \kappa)$. If $t \in \mathbf{T}$ acts on $\mathbf{U}$ then there is an induced action on $\mathfrak{u}$. The action on $\mathfrak{u}^*$ is then given by $t \cdot f(u) = f(t^{-1}u)$ for $f \in \mathfrak{u}^*$, $t \in T$ and $u \in \mathfrak{u}$.

This is immediately related to the action of G on an arbitrary representation usually denoted $\rho^x(g) = \rho(xgx^{-1})$ for any $x \in G$.

Proposition 5.2.4. *The action of G on ρ_Ω is given by $\rho_\Omega^g = \rho_{g^{-1}\Omega}$.*

Proof. Recall that

$$\rho_\Omega(h) = \frac{1}{(\text{card }\Omega)^{1/2}} \sum_{f\in\Omega} f(\log\ h) \qquad \forall h \in H.$$

Then,

$$\begin{aligned}
\rho_\Omega^g(h) &= \frac{1}{(\text{card }\Omega)^{1/2}} \sum_{f\in\Omega} f(\log\ ghg^{-1}) \\
&= \frac{1}{(\text{card }\Omega)^{1/2}} \sum_{f\in\Omega} g^{-1}f(\log\ h) \\
&= \frac{1}{(\text{card }\Omega)^{1/2}} \sum_{g^{-1}f} f(\log\ h).
\end{aligned}$$

for every $f \in \Omega$. □

Now, let S be the stabilizer of a representation ρ_Ω in G. We have $S \supset U$ because an inner automorphism always produces an isomorphic representation. Therefore, S/U is cyclic. By Lemma 5.2.3, for any Ω, we can find an irreducible representation ρ_Ω^1 so that its restriction to U is ρ_Ω. In particular, $\dim \rho_\Omega^1 = \dim \rho_\Omega$.

The set of irreducible K-representations of S is not always in one-to-one correspondence with the set of irreducible κ-representations. We begin with the "ordinary" K-representations.

5.2.1 Irreducible K-characters of G

Let S be the stabilizer of an irreducible K-character ρ_Ω of U. Since S/U is abelian and since K is sufficiently large, S/U has $|S/U|$ one dimensional K-representations.

Lemma 5.2.5. *Fix a lift ρ^1 of ρ_Ω. Then every irreducible component of $\text{ind}_U^S \rho_\Omega$ has the form $\sigma \otimes \rho^1$ for some irreducible character σ of S/U.*

Proof. Since

$$\langle \text{ind}_U^G \rho_\Omega, \sigma \otimes \rho^1 \rangle = \langle \rho_\Omega, \rho_\Omega \rangle = 1$$

by Frobenius reciprocity it is sufficient to show that $\sigma_1 \otimes \rho^1_\Omega$ and $\sigma_2 \otimes \rho^1_\Omega$ are pairwise non-isomorphic. This is exactly the corollary ascribed to Gallagher at [Isa94, Corollary 6.17]. □

Since every such $\sigma \otimes \rho^1$ is a choice of extension of ρ_Ω, it is reasonable to try to induce extensions from S to G. It turns out that we can find every irreducible representation of G from ind^G_S. More precisely:

Lemma 5.2.6. *Suppose ρ_Ω is an irreducible representation of U and ρ^1 is an extension of ρ_Ω in S. Then $\operatorname{ind}^G_S \rho^1_\Omega$ is irreducible.*

Proof. Let $\dim \rho_\Omega = n$. By Lemma 5.2.3 we have $\dim \rho^1_\Omega = n$. The dimension $\dim \operatorname{ind}^G_S \rho^1_\Omega = [G : S]n$. By Theorem 5.2.1 every irreducible KG-module whose restriction contains ρ_Ω must contain the full G orbit of ρ_Ω. Thus, $\operatorname{res}^G_U \operatorname{ind}^G_S \rho^1_\Omega$ has $\bigoplus \rho^{g_i}_\Omega$ as a sub-character where $\rho^{g_i}_\Omega$ are the distinct elements in the G orbit of ρ_Ω. However, the dimension of $\bigoplus \rho^{g_i}_\Omega$ is also $[G : S]n$, so $\operatorname{ind}^G_S \rho^1_\Omega$ is irreducible. □

This will give us every irreducible representation of G whose restriction contains a fixed ρ_Ω by the previous two lemmata. However, we can actually find *every* irreducible K-character in this way.

Theorem 5.2.7. *Every irreducible K-character of G is of the form $\operatorname{ind}^G_S \rho^1_\Omega$ for a fixed extension ρ^1_Ω of ρ_Ω to S.*

Proof. Suppose that α is an irreducible character of G. Let ρ_Ω be a constituent character of $\operatorname{res}^G_U \alpha$ and let S be the stabilizer of ρ_Ω in G. We will show that there exists a lift of ρ_Ω to S whose induced character to G is isomorphic to α. Consider $\operatorname{ind}^S_U \rho_\Omega$, which contains every extension ρ^1_Ω of ρ_Ω by

$$\langle \operatorname{ind}^S_U \rho_\Omega, \rho^1_\Omega \rangle = 1.$$

Since $\operatorname{res}^G_U \alpha$ has ρ_Ω as a constituent character we compute

$$\langle \operatorname{ind}^S_U \rho_\Omega, \operatorname{res}^G_S \alpha \rangle = \langle \rho_\Omega, \operatorname{res}^G_U \alpha \rangle \geq 1.$$

Thus, there exists at least one shared irreducible K-character ρ_Ω^1 which is a constituent of both $\operatorname{ind}_U^S \rho_\Omega$ and $\operatorname{res}_S^G \alpha$. Then $\operatorname{ind}_S^G \rho_\Omega^1$ is irreducible by the previous theorem and isomorphic to α by

$$\langle \alpha, \operatorname{ind}_S^G \rho_\Omega^1 \rangle = 1.$$

□

We can be fairly explicit with the structure of the regular representation: since K is algebraically closed and characteristic 0, the regular representation is semisimple with components as given.

It is also useful to describe the irreducible representations according to the dimension formula

$$|G| = \sum (\dim \alpha_i)^2$$

where α_i are all irreducible representations of G. Suppose ρ_1 to ρ_n are a complete set of irreducible characters of U with stabilizers S_1 to S_n. For each S_i there are $|S_i/U|$ irreducible characters of S_i/U, which we will call σ_i^j. The extensions $\sigma_i^j \otimes \rho_i^1$ give every irreducible character of S_i which restricts to ρ_i and have dimension equal to that of ρ_i.

Then $\operatorname{ind}_{S_i}^G \sigma_i^j \otimes \rho_i^1$ is irreducible and has dimension $|G/S_i| \dim \rho_i$. An induced representation necessarily contains other ρ_i, in particular, it contains exactly one G orbit $|G|/|S_i|$ of ρ_i which all have the same dimension. We can then sum over $m \leq n$ with

$$\sum_{i=1}^{n} \dim \rho_i^2 = \sum_{j=1}^{m} \frac{|G| \rho_j^2}{|S_j|} = |U|$$

where j indexes ρ_i which are not in the same G orbit. The dimension formula then gives

$$\sum_{j=1}^{m} |S_j/U| |G/S_j|^2 \dim \rho_j^2 = \frac{|G|}{|U|} \sum_{j=1}^{m} \frac{|G| \rho_j^2}{|S_j|} = |G|.$$

5.2.2 Irreducible κ-characters of G

Now, suppose that S is the stabilizer of an irreducible κ-character ρ_Ω of U. While S is the same as above, the number of irreducible κ-representations of the cyclic group S/U is smaller than the number of irreducible K representations: κ lacks ℓ^i-th roots of unity. Suppose $|S/U| = a\ell^m$ with a co-prime to ℓ. The irreducible characters of S/U then factor through the irreducible characters of a cyclic group C_a order a. In particular, if $A = S/H$ and B is the ℓ-primary subgroup of A, then the irreducible representations of A in characteristic ℓ are precisely the irreducible representations of A. Given a character $\chi : S/U \to \kappa^\times$, $\chi(x) = 1$ when the order of x divides ℓ^a.

However, there are noticeable similarities to the previous section.

Lemma 5.2.8. *Suppose that W is an irreducible representation of U with stabilizer S in G and that W^1 is a $\kappa[S]$-module with $\operatorname{res}_U^S W^1 = W$. Then $\operatorname{ind}_S^G W^1$ is an irreducible κG module.*

Proof. The proof is the same as the previous section. Given an extension W^1 of W, the dimension $|\operatorname{ind}_S^G W^1|$ is equal to the dimension of the direct sum of the G-orbit of W in U. Thus W^1 is irreducible. □

Theorem 5.2.1. *Every irreducible κ-representation of G is of the form $\operatorname{ind}_S^G M$ where M is an irreducible representation of S with the form $\operatorname{res}_U^S M \cong W$ for W an irreducible representation of U with stabilizer S.*

Proof. Suppose that A is an irreducible representation of G. Then res_U^G is semisimple, so choose a simple submodule W. We claim that A can be induced from the stabilizer S of W in G.

We check the group

$$\operatorname{Hom}(\operatorname{ind}_S^S W, \operatorname{res}_S^G A).$$

By Frobenius reciprocity,

$$\operatorname{Hom}(\operatorname{ind}_U^S W, \operatorname{res}_S^G A) \cong \operatorname{Hom}(W, \operatorname{res}_U^G A)$$

which implies there exists a nontrivial homomorphism from W to $\operatorname{res}_U^G A$. Therefore, there exists some composition factor M of $\operatorname{ind}_U^S W$ which is isomorphic to a submodule of $\operatorname{res}_S^G A$. Then, by Lemma 5.2.8, $\operatorname{ind}_S^G M$ is irreducible. Furthermore,

$$\operatorname{Hom}(\operatorname{ind}_S^G M, A) = \operatorname{Hom}(M, \operatorname{res}_S^G A)$$

which is nonzero by construction. Thus, since both $\operatorname{ind}_S^G M$ and A are irreducible, they are isomorphic. Since every composition factor of $\operatorname{ind}_U^S W$ has $\operatorname{res}_U^S M \cong W$, every irreducible representation of G arises as a lift of an irreducible representation W of U.

Every composition factor has $\operatorname{res}_U^S M \cong W$, so $\langle \operatorname{res}_S^G A, \operatorname{ind}_U^S W \rangle$ is nonzero. Let $U_1 \supset \ldots \supset U_n$ be a composition series for $\operatorname{ind}_U^S W$. Every composition factor has the form $\operatorname{res}_U^S U_i/U_{i+1} \cong W$. Then, existence of an element of $\operatorname{Hom}(\operatorname{res}_S^G A, \operatorname{ind}_U^S W)$ implies that there is a simple composition factor M which appears in both $\operatorname{res}_S^G A$ and $\operatorname{ind}_U^S W$.

Finally, $\operatorname{ind}_S^G M$ is irreducible in G by the previous lemma, so $\langle \operatorname{res}_S^G A, M \rangle \geq 1$ implies that

$$\langle A, \operatorname{ind}_S^G M \rangle = 1.$$

□

5.3 Example: Modular Representations of $H_\beta \rtimes T$

Let $T = \mathbf{F}_{p^2}^\times$ which is a cyclic group of order $p^2 - 1 = (p+1)(p-1)$. The group T has an action on H_β given by

$$a \cdot (g_1, g_2) = (ag_1, a^{p+1} g_2).$$

This action gives a nontrivial automorphism of H_β.

We would like to identify all of the orbits of this T action. When $g_1 \neq 0$, the orbit size is necessarily $p^2 - 1$ since g_1 will go to every nonzero element of $\mathbf{F}_q$. Now suppose $g_1 = 0$. The elements $(0, g_2)$ have a substantial stabilizer in T since T has a cyclic subgroup of order $p+1$.

There are exactly $p+1$ elements of $\mathbf{F}_{p^2}^{\times}$ with $a^{p+1} = 1$. Let $\phi : \mathbf{F}_{p^2} \to \mathbf{F}_{p^2}$ take $a \mapsto a^{p+1}$. Then $|\ker(\phi)| = p+1$, which means that $|\mathrm{im}(\phi)| = p-1$ by the first isomorphism theorem. This gives that there are $p-1$ elements in the T orbit of $(0, g_2)$.

The action of T on orbits in $\mathfrak{g}^*$ is also This gives that there are $p-1$ elements in the T orbit of $(0, g_2)$. The action of T on orbits in $\mathfrak{g}^*$ is also useful, useful, because

$$\rho_{\Omega}^{t}(g) = \rho_{t \cdot \Omega}(g).$$

When $v_2 \in \mathbf{F}_p$ then the singleton orbit (v_1, v_2) is glued by Clifford theory to $p^2 - 1$ other singleton orbits provided $v_1 \neq 0$: they will be contained in the restriction of the same irreducible character of $G = H_\beta \rtimes T$. When $v_1 = 0$, it is glued to $p-1$ other orbits if $v_2 \neq 0$ and no other orbits when $v_2 = 0$.

When $v_2 \notin \mathbf{F}_p$, the action of T on the first term does not matter because the other av_1 were already in the coadjoint orbit of H_β. Therefore, we only have to worry about the $p-1$ orbits that are glued together in the second term. The full chart is as follows

Element of $\mathfrak{g}^*$	Conditions	Total G orbit size	Number of orbits
$(0,0)$		1	1
$(0, v_2)$	$v_2 \in \mathbf{F}_p$	$p-1$	1
(v_1, v_2)	$v_1 \neq 0,\ v_2 \in \mathbf{F}_p$	$p^2 - 1$	p
$(0, v_2)$	$v_2 \notin \mathbf{F}_p$	$(p-1)(p^2)$	p

This accounts for all p^4 elements of H_β.

5.3.1 Clifford theory for $T \ltimes H_\beta$

Once we have knowledge of the T action on representations of H_β, we can use Clifford theory to construct the irreducible representations of $G = H_\beta \rtimes T$.

Let S be the stabilizer of a given representation ρ_ω in G. By Theorem 5.2.7 every irreducible representation of S can be induced to an irreducible representation of G.

For example, the representation $\rho_{(0,0)}$ has $S = G$. Then, by the lifting properties there are $p^2 - 1$ representations of G whose restriction is exactly $\rho_{(0,0)}$.

The stabilizer of $\rho_{(0,v_2)}$ in G with $v_2 \in \mathbf{F}_p$ must have order $(p+1)(p^4)$. Therefore, there are $p+1$ irreducible K-representations of S which contain the irreducible representation $\rho_{(0,v_2)}$ of H_β. Each of those representations can be induced up to G, and each of those induced representations is irreducible and has restriction

$$\operatorname{res}^G_{H_\beta} \operatorname{ind}^G_S \rho^1_{(0,v_2)} = \sum_{T \text{ orbit}} \rho^t_{(0,v_2)}.$$

This is a representation of dimension $p-1$, so we are done.

In the same way, each of the $\rho_{(v_1,v_2)}$ lifts to one representation of dimension p^2-1. Each $\rho_{(0,v_2)}$ with $v_2 \notin \mathbf{F}_p$ is a p-dimensional representation in H_β, so it lifts to $p+1$ representations of dimension $(p-1)p$. This is all of the irreducible K-representations of G, a fact which we can be verified by the dimension formula.

Chapter 6

A Bound on Cohomology

Given a reductive group G, and a rational representation $G \to \mathrm{GL}(V)$, we know that $H^i(G,V) = H^i(B,V)$ for a Borel subgroup $B \subset G$. Then, with $B = T \ltimes U$ since $H^i(B,V) = H^i(U,V)^T$, we can exploit the T module structure of $k[U]$ to find an upper bound for the dimension of $H^i(G,V)$ based only on the action of T on V.

6.1 Introduction

Let k be an algebraically closed field with $\mathrm{char}(k) \geq 2$. Let B be a connected solvable group with T a maximal torus and $U = R_u B$. Let $\mu_1, \ldots, \mu_e$ be the weights of T on $\mathrm{Lie}(U)$. Consider the following condition on the μ_i:

If a_i are non-negative integers then

$$\sum_{i=1}^{e} a_i \mu_i = 0 \text{ implies that all of the } a_i = 0. \tag{6.1}$$

We will prove the following theorem:

Theorem 6.1.1. *Let B be a connected solvable group with maximal torus T where condition (6.1) holds. If V is an n-dimensional B-module then*

$$\dim H^i(B,V) \leq n M^i(B,\lambda)$$

for a weight λ of V and $M^i(B,\lambda)$ an integer described below.

To prove this, we will first look at the algebraic group W which is a vector group - isomorphic to a product of additive groups - and a torus T with an action on W. We first look at the Hochschild complex

$$C^i(G,M) = M \otimes \bigotimes^{i} k[G].$$

We describe this complex along with connecting maps ∂^i in Definition 2.3.3. The cohomology $H^n(G,M)$ is $\ker(\partial^{i+1})/\operatorname{im}(\partial^i)$. For the purposes of this chapter, we only need the definition of the complex itself and that $\dim H^i(G,V) \leq \dim C^i(G,V)$.

Since the terms of the complex $C^i(W,k_\lambda)$ are all T modules, we have a T action. The dimension of the torus fixed points of this complex is exactly the weight 0 space. Then, computing this dimension reduces to a combinatorial question: for a fixed λ, how many ways are there to arrange polynomials in $\bigotimes^i k[W]$ so that the weights add to λ?

Once there is a bound on $C^i(W,k_\lambda)^T$, we can use the same bound on to torus fixed points of arbitrary unipotent groups and finally to connected solvable groups. This gives an explicit, large, upper bound on cohomology $H^i(B,k_\lambda)$, which we can extend to $H^i(B,V)$ using only first principles. A theorem in [Jan03] gives the nice corollary:

Corollary 6.1.2. *For a reductive group G and an n-dimensional T-module V,*

$$H^i(G,V) \leq nM^i(G,\lambda)$$

for some weight λ of V and $M^i(G,\lambda)$ as described below.

6.2 Group Actions on the Hochschild complex

Let $\operatorname{char}(k) \geq 2$. We first look at torus fixed points in $C^i(U,k)$. It will benefit us to look at a short example before we begin.

Example 6.2.1. Let W be an a dimensional T-module with its T-module structure given by $t \cdot w = \mu(t)w$ for all $w \in W$ and $t \in T$ with $\mu \neq 0$. We are going to use the algebraic group structure on W, so we view it as a product of a additive groups.

We would like to find the dimension of the zero weight space of $C^i(W,k_\lambda)$ for arbitrary λ. If $\lambda \neq b\mu$ for any b then there is nothing in the zero weight space.

Now we examine the dimension of $C^1(W,k_\lambda)^T$ if $\lambda = b\mu$ for some positive integer b. The basis for the degree b homogeneous functions in $k[W]$ each give a torus fixed point in C^1 since an element will have weight $b\mu$.

Now, degree b homogeneous elements of $C^i(W,k_\lambda)^T$ come from elements of

$$k[T]_{c_1} \otimes \cdots \otimes k[T]_{c_i} \qquad \text{with} \qquad c_1 + \cdots + c_i = b.$$

However, it is easier to look at all of our variables at once by checking $k[T \times \cdots \times T]_b$. Then, we only have to count the number of ways we can partition b over ia different variables. This corresponds to the number of ways to write $x_1 + x_2 + \cdots + x_{ia_i - 1} + x_{ia_i} = b$ where x_i are non-negative integers. This is the well known "stars and bars" problem, so we have the well known solution

$$\dim C^i(W,k_\lambda)^T \leq \binom{b + ia - 1}{ia - 1}.$$

The number of ways to write a weight as a non-negative sum of roots in a given root system is called the Konstant partition function. It is well known that the Konstant partition function is finite, but a proof of the following remark is provided:

Proposition 6.2.2. *Suppose λ is a weight and $\mu_1, \dots, \mu_e$ have the property that*

$$\sum_{i=1}^{e} a_i \mu_i = 0$$

for non-negative integers a_i implies that all the $a_i = 0$. Then there are finitely many sets $(b_1, \dots, b_i)$ for which $b_1\mu_1 + \cdots + b_i\mu_i = \lambda$.

Proof. Suppose that $\mu_1, \dots, \mu_e$ have the property that for any integers a_i which are non-negative we have that

$$a_1\mu_1 + \cdots + a_e\mu_e = 0$$

implies that all the a_i are 0. Call $\mathcal{B}$ the set of vectors $b = [b_1, \dots, b_e]$ for which

$$\lambda = b_1\mu_1 + \cdots + b_e\mu_e$$

and suppose that $\mathcal{B}$ is infinite. Fix $[a_1, \dots, a_e] \in \mathcal{B}$ and let

$$\sum_{i=1}^{e} a_i = M.$$

The number of tuples $[b_1, \dots, b_e]$ whose entries sum to M correspond to a partition of M into e parts. There are therefore finitely many tuples of non-negative integers whose entries sum to a given number M.

There must be a vector in $b \in \mathcal{B}$ with $b_i \geq a_i$ for all i and $b_j > a_j$ for some j. Then

$$0 = \lambda - \lambda = \sum_{i=1}^{e} (b_i - a_i)\mu_i$$

is a positive linear combination of the μ_i, which implies that $b_i - a_i$ must be 0. Thus there are only finitely many $b \in \mathcal{B}$. □

The following lemma contains the bulk of the content of the main theorem of this chapter:

Lemma 6.2.3. *Let W be a product of additive groups seen as a T-module with positively linearly independent weights $\mu_1, \dots, \mu_e$ whose weight spaces have dimension $a_1, \dots, a_e$. Suppose $\lambda = \mu_1^{b_1} \cdots \mu_e^{b_e}$ for all $b = [b_1, \dots, b_e]$ in a finite set $\mathcal{B}$. Then*

$$\dim C^i(W, k_\lambda)^T \leq \sum_{b \in \mathcal{B}} \prod_{j=1}^{e} \binom{b_j + ia_j - 1}{ia_j - 1}.$$

Proof. Let

$$k[W] = k[X_{1,1}, \dots, X_{1,a_1}, \dots, X_{e,1}, \dots, X_{e,a_e}]$$

where $t \cdot X_{j,a_j} = \mu_j(t) X_{j,a_j}$. Fix $b \in \mathcal{B}$ so that $\lambda = \mu_1^{b_1} \cdots \mu_e^{b_e}$. Then $C^i(W, k_\lambda)^T$ are the elements in $k_\lambda \otimes k[W] \otimes \cdots \otimes k[W]$ where the sum of the powers of X_{j,a_j} across all components adds to b_j.

Then, the total number of ways this can happen is the product from 1 to e of the result from the example. Since we have this bound for each b in $\mathcal{B}$, all that remains is to add that bound so

$$\dim C^i(W, k_\lambda)^T \le \sum_{b\in\mathcal{B}} \prod_{j=1}^{e} \binom{b_j + ia_j - 1}{ia_j - 1}.$$

□

Since $H^i(W, k_\lambda)$ is a quotient of $C^i(W, K_\lambda)$, this is also a bound on the dimension of $H^i(W, k_\lambda)$. For the remainder of the paper we call this bound $M^i(W, \lambda)$.

6.3 Equality of Coordinate Rings

Proposition 6.3.1. *Let T act on G, a connected unipotent linear algebraic group. Then as T-modules,*

$$k[U] \cong k[\mathrm{Lie}(U)].$$

Proof. Since $\mathrm{Lie}(U)$ is a vector space, $k[\mathrm{Lie}(U)] = k[T_1, \ldots, T_d]$ where d is the dimension of $\mathrm{Lie}(U)$. We now show that as a T-module, $k[U]$ can be given the same structure.

Let $A = k[U]$ and let $\mathfrak{m}$ be the maximal ideal in A associated to 1 in U. For any T-module W with filtration

$$W = W_0 \supset W_1 \supset \cdots$$

with $\bigcap W_i = \{0\}$ then

$$W \cong \frac{W_0}{W_1} \oplus \frac{W_1}{W_2} \oplus \frac{W_2}{W_3} \oplus \cdots.$$

Then, as a T-module, $k[U]$ has a filtration of T-modules

$$A \supset \mathfrak{m} \supset \mathfrak{m}^2 \supset \mathfrak{m}^3 \supset \cdots$$

with $\bigcap \mathfrak{m}^i = \{0\}$. Thus

$$A \cong \frac{A}{\mathfrak{m}} \oplus \frac{\mathfrak{m}}{\mathfrak{m}^2} \oplus \cdots$$

so A is isomorphic to its associated graded ring $Gr_{\mathfrak{m}}$ as a T-module. Now, we use the following theorem from commutative algebra to finish the proof:

Theorem 6.3.2. *[AM69, Theorem 11.22] Let A be a Noetherian local ring of dimension d, $\mathfrak{m}$ its maximal ideal and $k = A/\mathfrak{m}$ Then the following are equivalent:*

i. $Gr_{\mathfrak{m}}(A) \cong k[t_1, \dots, t_d]$ *where the t_i are independent indeterminants;*

ii. $dim_k(\mathfrak{m}/\mathfrak{m}^2) = d$.

But $\mathfrak{m}/\mathfrak{m}^2$ is the Zariski cotangent space, so it also has dimension d. Thus as a T module, A is isomorphic to a polynomial ring of dimension d, so

$$k[U] \cong k[\mathrm{Lie}(U)].$$

□

As a direct corollary,

$$k_\lambda \otimes \bigotimes^{i} k[\mathrm{Lie}(U)] \cong C^i(U, k_\lambda),$$

so

$$\dim H^i(U, k_\lambda)^T \leq \dim C^i(U, k_\lambda)^T \leq M^i(\mathrm{Lie}(U), \lambda).$$

Now, since $H^i(U, k_\lambda)^T = H^i(B, k_\lambda)$, we have a bound on the cohomology of B. For convenience we will rename

$$M^i(\mathrm{Lie}(U), \lambda) = M^i(B, \lambda).$$

6.4 A Bound on $\dim H^i(B, V))$

We examine the exact sequence

$$0 \longrightarrow k_\lambda \longrightarrow V \longrightarrow V/k_\lambda \longrightarrow 0\ .$$

This gives a long exact sequence in cohomology

$$\cdots \longrightarrow H^i(B, k_\lambda) \longrightarrow H^i(B, V) \longrightarrow H^i(B, V/k_\lambda) \longrightarrow \cdots .$$

Now, if V has dimension 2 and has weights λ_1 and λ_2, we have that

$$\cdots \longrightarrow H^i(B, k_{\lambda_1}) \longrightarrow H^i(B, V) \longrightarrow H^i(B, k_{\lambda_2}) \longrightarrow \cdots$$

so the dimension of $H^i(B, V)$ is bounded above by $M^i(B, \lambda_1) + M^i(B, \lambda_2)$. Rename the weight with the larger M^i to α so that $\dim H^i(B, V) \leq 2M^i(B, \alpha)$.

Now, suppose that for any $n-1$-dimensional vector space W we have

$$H^i(B, W) \leq (n-1)M^i(B, \beta)$$

for some weight β. Then for an n-dimensional vector space V we have

$$\cdots \longrightarrow H^i(B, k_\lambda) \longrightarrow H^i(B, V) \longrightarrow H^i(B, W) \longrightarrow \cdots$$

so

$$\dim H^i(B, V) \leq (n-1)M^i(B, \beta) + M^i(B, \lambda).$$

Thus, if we replace the weight with the higher bound by α, we have

$$\dim H^i(B, V) \leq nM^i(B, \alpha).$$

If G is a reductive group with a rational representation $G \to GL(V)$ for an n-dimensional vector space V and B is a Borel subgroup of G with $B = T \ltimes U$, then $H^i(B, V)$ is bounded by $nM^i(B, \alpha)$ as in the sections above and [Jan03] by

$$H^i(B, V) = H^i(G, V).$$

Therefore, $H^i(G, V)$ has an upper bound based on the torus action T on V.

Appendix A

Proof of Theorem 3.2.6

Lemma A.0.1. *The group* $\mathrm{Ext}(W_n^{\mathrm{perf}}, \mathbf{G}_a^{\mathrm{perf}})$ *is a free left* A_1*-module with basis* α_n^1*.* $\mathrm{Ext}(\mathbf{G}_a^{\mathrm{perf}}, W_n^{\mathrm{perf}})$ *is a free right* A_1 *module with basis* α_1^n*.*

Proof. We first do the left A_1-module case. The right A_1 module argument is essentially the same but uses a different exact sequence of Ext.

We can use induction on the length of the truncated perfectized Witt vectors. Lemma 3.2.4 gives the base case. For $n \geq 2$, we need to use the exact sequence of Ext associated to the extension

$$0 \longrightarrow \mathbf{G}_a^{\mathrm{perf}} \xrightarrow{V^{n-1}} W_n^{\mathrm{perf}} \xrightarrow{R} W_{n-1}^{\mathrm{perf}} \longrightarrow 0$$

is given by

$$\mathrm{Ext}(W_{n-1}^{\mathrm{perf}}, \mathbf{G}_a^{\mathrm{perf}}) \xrightarrow{\lambda} \mathrm{Ext}(W_n^{\mathrm{perf}}, \mathbf{G}_a^{\mathrm{perf}}, \mathbf{G}_a^{\mathrm{perf}}) \xrightarrow{\mu} \mathrm{Ext}(\mathbf{G}_a^{\mathrm{perf}}, \mathbf{G}_a^{\mathrm{perf}}) \ .$$

If $x \in \mathrm{Ext}(W_{n-1}^{\mathrm{perf}}, \mathbf{G}_a^{\mathrm{perf}})$ we have $\lambda(x) = R^*(x) = xR$ and $\mu(y) = V^{(n-1)*}(y) = yV^{n-1}$ so λ and μ are homomorphisms for the structure of a left A_1 module.

We have the identities

$$V\alpha_n^m = \alpha_{n-1}^{m+1}R \qquad \text{and} \qquad \alpha_n^m V = \alpha_{n-1}^m$$

so $\lambda(\alpha_{n-1}^1) = \alpha_{n-1}^1 R = \alpha_n^0 = 0$. The induction hypothesis says that α_{n-1}^1 generates $\mathrm{Ext}(W_{n-1}^{\mathrm{perf}}, \mathbf{G}_a^{\mathrm{perf}})$, so $\lambda = 0$. Thus μ is injective.

By the same identities $\mu(\alpha_n^1) = \alpha_n^1 V^{n-1} = \alpha_1^1$ and, according to Lemma 3.2.4 α_1^1 is a basis of $\mathrm{Ext}(\mathbf{G}_a^{\mathrm{perf}}, \mathbf{G}_a^{\mathrm{perf}})$ so μ is surjective. It follows that μ is bijective and that α_n^1 is a basis of $\mathrm{Ext}(W_n^{\mathrm{perf}}, \mathbf{G}_a^{\mathrm{perf}})$.

For the right A_1 module case we also argue by induction with the exact sequence

$$0 \longrightarrow W_{n-1}^{\mathrm{perf}} \xrightarrow{V} W_n^{\mathrm{perf}} \xrightarrow{R^{n-1}} \mathbf{G}_a^{\mathrm{perf}} \longrightarrow 0$$

and the associated second exact sequence of Ext

$$\mathrm{Ext}(G_a^{\mathrm{perf}}, W_{n-1}^{\mathrm{perf}}) \xrightarrow{\lambda} \mathrm{Ext}(\mathbf{G}_a^{\mathrm{perf}}, W_n^{\mathrm{perf}}) \xrightarrow{\mu} \mathrm{Ext}(\mathbf{G}_a^{\mathrm{perf}}, \mathbf{G}_a^{\mathrm{perf}}) \ .$$

Then $\lambda(x) = V_*(x) = Vx$ and $\mu(y) = R_*^{n-1}(y) = R^{n-1}y$. We check $\lambda(\alpha_1^{n-1}) = \alpha_0^n = 0$ so λ is the zero map by the induction hypothesis.

The identity

$$R\alpha_n^m = \alpha_n^{m-1}$$

gives $\mu(\alpha_1^n) = R^{n-1}\alpha_1^n = \alpha_1^1$. Since α_1^1 is a basis of $\mathrm{Ext}(\mathbf{G}_a^{\mathrm{perf}}, \mathbf{G}_a^{\mathrm{perf}})$ on the as a left module as well, μ is surjective and α_1^n is a basis of $\mathrm{Ext}(\mathbf{G}_a^{\mathrm{perf}}, W_n^{\mathrm{perf}})$. □

Lemma A.0.2. *Let $n \geq 0$. For every $\phi \in A_1$, there exist Φ and Φ' in A_{n+1} so that $\phi R^n = R^n \Phi$ and $\Phi' V^n = V^n \phi$.*

Proof. We restrict to the case where $\phi(t) = \lambda t^{p^i}$ with $\lambda \in k$ and $i \in \mathbf{Z}$ and then extend linearly. Choose $w \in W_{n+1}^{\mathrm{perf}}$ so that $R^n w = \lambda$ and define Φ by the formula

$$\Phi(x) = w.F^i(x)$$

with product given by the product in W_{n+1}. Then

$$R^n\Phi(x) = \lambda.R^n F^i(x) = \lambda.F^i R^n(x) = \phi R^n(x).$$

Similarly, define Φ' by the formula

$$\Phi'(x) = w'.F^i(x), \qquad \text{with} \qquad R^n F^n w' = \lambda.$$

□

Lemma A.0.3. *Every element x of* $\mathrm{Ext}(W_n^{\mathrm{perf}}, \mathbf{G}_a^{\mathrm{perf}})$ *can be written* $x = \alpha_n^1 f$, *with* $f \in A_n$. *One has* $\alpha_n^1 f = 0$ *if and only if f is not an isogeny. Every element x of* $\mathrm{Ext}(\mathbf{G}_a^{\mathrm{perf}}, W_n^{\mathrm{perf}})$ *can be written* $x = g\alpha_1^n$, *with* $g \in A_n$. *One has* $g\alpha_1^n = 0$ *if and only if g is not an isogeny.*

Proof. We have $xV^{n-1} \in \mathrm{Ext}(\mathbf{G}_a^{\mathrm{perf}}, \mathbf{G}_a^{\mathrm{perf}})$. Then, Lemma 3.2.4 gives

$$xV^{n-1} = \alpha_1^1 \psi$$

with $\psi \in A_1$. By Lemma A.0.2, there exists $f \in A_n$ so that $fV^{n-1} = V^{n-1}\psi$ which immediately gives

$$xV^{n-1} = \alpha_1^1 \psi = \alpha_n^1 V^{n-1} \psi = \alpha_n^1 f V^{n-1}$$

However, $\mu : x \mapsto xV^{n-1}$ is bijective. The relation $xV^{n-1} = \alpha_n^1 f V^{n-1}$ then implies that $x = \alpha_n^1 f$.

We also have that $x = 0$ is the same statement as $xV^{n-1} = 0$. The previous lemma then gives $\alpha_1^1 \psi = 0$ and $\psi = 0$. By $fV^{n-1} = V^{n-1}\psi$, $fV^{n-1} = 0$. This gives that the kernel of f contains an additive group, so it is positive dimensional. Similar manipulations give the other half of the lemma. Start with $R^{n-1}x \in \mathrm{Ext}(\mathbf{G}_a^{\mathrm{perf}}, \mathbf{G}_a^{\mathrm{perf}})$ which gives

$$R^{n-1}x = \psi \alpha_1^1$$

for some $\psi \in A_1$. According to Lemma A.0.2 there exists $g \in A_n$ so that $R^{n-1}g = \psi R^{n-1}$ which gives

$$R^{n-1}x = \psi \alpha_1^1 = \psi R^{n-1} \alpha_1^n = R^{n-1} g \alpha_1^n.$$

A homomorphism $\mu : x \mapsto R^{n-1}x$ is also bijective so the relation $R^{n-1}x = R^{n-1}g\alpha_1^n$ implies that $x = g\alpha_1^n$. When $x = 0$, $\psi = 0$ by the analogous argument to above. Equivalently $R^{n-1}f = 0$ and the kernel of g is also positive dimensional. □

Lemma A.0.4. *If $m \geq n$, every element* $x \in \mathrm{Ext}(W_n^{\mathrm{perf}}, \mathbf{G}_a^{\mathrm{perf}})$ *can be written* $x = \alpha_m^n f$ *with* $f \in \mathrm{Hom}(W_n^{\mathrm{perf}}, W_m^{\mathrm{perf}})$. *If $m \geq n$, every element* $x \in \mathrm{Ext}(\mathbf{G}_a^{\mathrm{perf}}, W_n^{\mathrm{perf}})$ *can be written* $x = g\alpha_1^m$ *with* $g \in \mathrm{Hom}(W_m^{\mathrm{perf}}, W_n^{\mathrm{perf}})$.

Proof. According to Lemma A.0.3, $x = \alpha_n^1 f_1$ with $f_1 \in A_n$. As $\alpha_n^1 = \alpha_m^1 V^{m-n}$, this can be written $x = \alpha_m^1 V^{m-n} f_1$ and we put $f = V^{m-n} f_1$ which is an element of $\mathrm{Hom}(W_n^{\mathrm{perf}}, W_m^{\mathrm{perf}})$. The proof of the second half is analogous with $g = g_1 R^{m-n}$. □

A.1 Isogenies with a product of Witt Groups

Let G be a connected unipotent perfect group scheme. Every element x of $\mathbf{G}_a^{\mathrm{perf}}$ is p-torsion because every element of $\mathbf{G}_a$ is p-torsion. Thus, because G is a multiple extension of groups $\mathbf{G}_a^{\mathrm{perf}}$, there exists an integer $n \geq 0$ such that $p^n.x = 0$ for all $x \in G$. The *period* of G is the smallest power of p satisfying this condition. In particular, if $n = \dim G$, the period of G is less than or equal to p^n. On the other hand

Proposition A.1.1. *Let G be a commutative connected unipotent group of dimension n. The following three conditions are equivalent.*

(i) The period of G is equal to p^n

(ii) There exists an isogeny $f : W_n^{\mathrm{perf}} \to G$

(ii)' There exists an isogeny $f' : G \to W_n^{\mathrm{perf}}$

Proof. Since the period is invariant by isogeny, the implications from $(ii) \Rightarrow (i)$ and $(ii)' \Rightarrow (i)$ are immediate. We can use induction for $(i) \Rightarrow (ii)$. If $n = 1$, this group is trivial. If $n \geq 2$, G can be is an extension of a group G_1 of dimension $n-1$ by the group $\mathbf{G}_a^{\mathrm{perf}}$. The period of G_1 is necessarily p^{n-1}, and the induction hypothesis says there exists an isogeny $g : W_{n-1} \to G_1$. Then $g^*(G) \in \mathrm{Ext}(W_{n-1}^{\mathrm{perf}}, \mathbf{G}_a^{\mathrm{perf}})$ and by Lemma A.0.1 there exists $\phi \in A_1$ so that $g^*(G) = \phi_*(W_n^{\mathrm{perf}})$. By definition, this says there exists a homomorphism $f : W_n \to G$ making a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbf{G}_a^{\mathrm{perf}} & \longrightarrow & W_n^{\mathrm{perf}} & \longrightarrow & W_{n-1}^{\mathrm{perf}} & \longrightarrow & 0 \\ & & \downarrow \phi & & \downarrow f & & \downarrow g & & \\ 0 & \longrightarrow & \mathbf{G}_a^{\mathrm{perf}} & \longrightarrow & G & \longrightarrow & G_1 & \longrightarrow & 0 \end{array}.$$

If ϕ were equal to 0 the homomorphism g would define by passage to the quotient a homomorphism from W_{n-1} to G and the group G would be isogenous to $\mathbf{G}_a \times W_{n-1}$ and we would be done. But, since g is an isogeny, the same is true of f which proves $(i) \Rightarrow (ii)$. The implication $(i) \Rightarrow (ii)'$ has the same proof using the second part of Lemma A.0.1. □

Proposition A.1.2. *Let* $W = \prod W_{n_i}^{\text{perf}}$ *be a product of perfectized Witt groups, and let* G *be a connected unipotent group. The following conditions are equivalent:*

(i) There exists an isogeny $f : G \to W$

(i)' There exists an isogeny $g : W \to G$*.*

Proof. Suppose that (i) is true and let G_i' be the inverse images in G of the factors $W_{n_i}^{\text{perf}}$ in W; for every i let G_i be the connected component of the identity of G_i'. The map $f_i : G_i \to W_{n_i}^{\text{perf}}$ defined by f is an isogeny. According to A.1.1, there exists an isogeny $G_i : W_{n_i}^{\text{perf}} \to G_i$ and the map $g : W \to G$ which is the sum of the g_i is an isogeny, which proves $(a) \Rightarrow (a)'$. The other direction from $(a)' \Rightarrow (a)$ is similar. □

Proof. Suppose that G is a connected unipotent perfect group scheme of dimension r. We argue by induction on r, with $r = 1$ referring to isogenies of the additive group. The group G is an extension of a group G_1 of dimension $r-1$ by the group G_a^{perf}. The induction hypothesis is that there exists an isogeny

$$f : \prod_{i=1}^{i=k} W_{n_i} \to G_1.$$

Put $W = \prod_{i=1}^{i=l} W_{n_i}^{\text{perf}} \to G_1$. The group $f^*(G)$ is an extension of W by $\mathbf{G}_a^{\text{perf}}$ and is isogenous to G. Then, if G is a product of Witt groups we are done.

In this case, the extension G is then defined by a family of elements γ_i which are in $\text{Ext}(W_{n_i}^{\text{perf}}, \mathbf{G}_a^{\text{perf}})$. Suppose $n_1 \geq n_i$ for all i and let W' be the product of the W_{n_i} starting at the second term $i \geq 2$. We treat γ_1 differently depending on if it is trivial factor system or not:

1. If $\gamma_1 = 0$, G is immediately a product of W_n, and the extension of W' by $\mathbf{G}_a$ is defined by the system (γ_i) for $i \geq 2$. The induction hypothesis shows that G is isogenous to a product of Witt groups.

2. If $\gamma_1 \neq 0$ we can define a different extension. Suppose $\beta = (\beta_i) \in \mathrm{Ext}(W, \mathbf{G}_a^{\mathrm{perf}})$ is the element defined by $\beta_1 = \alpha_n^1$ and $\beta_i = 0$ if $i \geq 2$. The extension G' corresponding to β is exactly the product $W_{n_{i+1}} \times W'$. Then, an isogeny exists from W to W exists. Let $\phi : W \to W$ so that $\phi^*(G')$ is isomorphic to G. It will follow that G is isogenous to G', which is a product of Witt groups.

   According to Lemma A.0.4, there exists $f_i \in \mathrm{Hom}(W_{n_i}^{\mathrm{perf}}, W_n^{\mathrm{perf}})$ such that $\gamma_i = \alpha_n^1 f_i$. Thus we define $\phi : W \to W$ by the formula

   $$\phi(w_1, w_2, \dots, w_k) = (f_1(w_1) + \dots + f_k(w_k), w_2, \dots, w_k).$$

   Then, $\phi^*(\beta) = \gamma$ where γ can be seen as an element of $\mathrm{Ext}(W, G_a^{\mathrm{perf}})$ associated to G. We have that f_1 is surjective by Lemma A.0.3 which gives $\alpha_n^1 f_1 \neq 0$. Therefore, ϕ is also surjective and it is an isogeny.

□

Proof. Let G be such a group and let r be its dimension. When $r = 1$, any commutative connected unipotent group is isomorphic to a subgroup given by an isogeny of $\mathbf{G}_a$ to $\mathbf{G}_a$ or given by the quotient by the trivial group. Suppose G is an extension of $\mathbf{G}_a^{\mathrm{perf}}$ by a group of G_1 of dimension $r - 1$. By induction hypothesis, G_1 can be embedded in a product W of Witt groups, and G can be embedded in the corresponding extension of $\mathbf{G}_a^{\mathrm{perf}}$ by W.

Now, let $W = \prod_{i=1}^{u=m} W_{n_i}$ be a decomposition of W into a product of Witt groups. An element $G \in \mathrm{Ext}(\mathbf{G}_a^{\mathrm{perf}}, W)$ is defined by a family of elements $\gamma_i \in \mathrm{Ext}(\mathbf{G}_a, W_{n_i})$. According to Lemma A.0.1, there exists $\phi_i \in A_1$ such that $\gamma_i = \alpha_1^{n_i} \phi_i$. Then put

$$L = \prod_{i=1}^{i=m} W_{n_i+1} \times \mathbf{G}_a^{\mathrm{perf}}.$$

We can consider L as an extension of $(\mathbf{G}_a^{\text{perf}})^m \times \mathbf{G}_a^{\text{perf}}$ by W; let

$$\beta \in \operatorname{Ext}((\mathbf{G}_a^{\text{perf}})^m \times \mathbf{G}_a^{\text{perf}}, W_{n_i})$$

be the corresponding element. Then we define a homomorphism

$$\theta : \mathbf{G}_a^{\text{perf}} \to (\mathbf{G}_a^{\text{perf}})^m \times \mathbf{G}_a$$

by the formula

$$\theta(x) = (\phi_1(x), \ldots, \phi_m(x), x).$$

We have then that $\beta\theta = G$ which corresponds to the existence of a homomorphism $\psi : G \to L$ making a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & W & \longrightarrow & G & \longrightarrow & \mathbf{G}_a^{\text{perf}} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow \psi & & \downarrow \theta & & \\ 0 & \longrightarrow & W & \longrightarrow & L & \longrightarrow & (\mathbf{G}_a^{\text{perf}})^m \times \mathbf{G}_a & \longrightarrow & 0 \end{array}.$$

That means that θ is an embedding of $\mathbf{G}_a^{\text{perf}}$ in $(\mathbf{G}_a^{\text{perf}})^m \times \mathbf{G}_a^{\text{perf}}$. The same is therefore also true for ψ which finishes the proof.

We argue by induction on the dimension of the given group G, by considering G as an extension of a group G_1 by $\mathbf{G}_a^{\text{perf}}$. The induction hypothesis can be applied to G_1, which means we can suppose that G_1 is a product $\prod_{i=1}^{i=m} W_{n_i+1}^{\text{perf}} \times \mathbf{G}_a^{\text{perf}}$ of Witt groups. Then, G is isomorphic to the quotient of $\prod_{i=1}^{i=m} W_{n+1}^{\text{perf}} \times \mathbf{G}_a^{\text{perf}}$ by a connected subgroup isomorphic to $(\mathbf{G}_a^{\text{perf}})^m$ □

Bibliography

[AM69] M. F. Atiyah and I. G. Macdonald. *Introduction to commutative algebra*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969.

[BD06] Mitya Boyarchenko and Vladimir Drinfeld. A motivated introduction to character sheaves and the orbit method for unipotent groups in positive characteristic, 2006.

[BD14] Mitya Boyarchenko and Vladimir Drinfeld. Character sheaves on unipotent groups in positive characteristic: foundations. *Selecta Math. (N.S.)*, 20(1):125–235, 2014.

[Boy07] Dmitriy Sergeyevich Boyarchenko. *Characters of unipotent groups over finite fields*. ProQuest LLC, Ann Arbor, MI, 2007. Thesis (Ph.D.)–The University of Chicago.

[Boy10] Mitya Boyarchenko. Characters of unipotent groups over finite fields. *Selecta Math. (N.S.)*, 16(4):857–933, 2010.

[Boy13] Mitya Boyarchenko. Character sheaves and characters of unipotent groups over finite fields. *Amer. J. Math.*, 135(3):663–719, 2013.

[CR06] Charles W. Curtis and Irving Reiner. *Representation theory of finite groups and associative algebras*. AMS Chelsea Publishing, Providence, RI, 2006. Reprint of the 1962 original.

[DBFPS08] Alfonso Di Bartolo, Giovanni Falcone, Peter Plaumann, and Karl Strambach. *Algebraic groups and Lie groups with few factors*, volume 1944 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2008.

[DF04] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[Gre65] Marvin J. Greenberg. Perfect closures of rings and schemes. *Proceedings of the American Mathematical Society*, 16(2):pp. 313–317, 1965.

[Gro60] A. Grothendieck. éléments de géométrie algébrique. I. Le langage des schémas. *Inst. Hautes Études Sci. Publ. Math.*, page 228, 1960.

[Isa94] I. Martin Isaacs. *Character theory of finite groups*. Dover Publications, Inc., New York, 1994. Corrected reprint of the 1976 original [Academic Press, New York; MR0460423 (57 #417)].

[Jan03] Jens Carsten Jantzen. *Representations of algebraic groups*, volume 107 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, second edition, 2003.

[Lan84] Serge Lang. *Algebra*. Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, second edition, 1984.

[Lus85] George Lusztig. Character sheaves. I. *Adv. in Math.*, 56(3):193–237, 1985.

[McN02] George J. McNinch. Abelian unipotent subgroups of reductive groups. *J. Pure Appl. Algebra*, 167(2-3):269–300, 2002.

[McN10] George J. McNinch. Levi decompositions of a linear algebraic group. *Transform. Groups*, 15(4):937–964, 2010.

[McN14] George J. McNinch. Linearity for actions on vector groups. *J. Algebra*, 397:666–688, 2014.

[Mum88] David Mumford. *The red book of varieties and schemes*, volume 1358 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1988.

[Mum14] David Mumford. Can one explain schemes to biologists, 2014.

[Ros56] Maxwell Rosenlicht. Some basic theorems on algebraic groups. *Amer. J. Math.*, 78:401–443, 1956.

[Ser77] Jean-Pierre and Serre. *Linear representations of finite groups*. Springer-Verlag, New York-Heidelberg, 1977. Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.

[Ser79] Jean-Pierre and Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[Ser88] Jean-Pierre Serre. *Algebraic groups and class fields*, volume 117 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1988. Translated from the French.

[Spr98] T. A. Springer. *Linear algebraic groups*, volume 9 of *Progress in Mathematics*. Birkhäuser Boston, Inc., Boston, MA, second edition, 1998.

[Wei94] Charles A. Weibel. *An introduction to homological algebra*, volume 38 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1994.