ABELIAN UNIPOTENT SUBGROUPS OF REDUCTIVE GROUPS

GEORGE J. MCNINCH

ABSTRACT. Let G be a connected reductive group defined over an algebraically closed field k of characteristic $p > 0$. The purpose of this paper is two-fold. First, when p is a good prime, we give a new proof of the "order formula" of D. Testerman for unipotent elements in G; moreover, we show that the same formula determines the p-nilpotence degree of the corresponding nilpotent elements in the Lie algebra $\mathfrak{g}$ of G.

Second, if G is semisimple and p is sufficiently large, we show that G always has a faithful representation (ρ, V) with the property that the exponential of $d\rho(X)$ lies in $\rho(G)$ for each p-nilpotent $X \in \mathfrak{g}$. This property permits a simplification of the description given by Suslin, Friedlander, and Bendel of the (even) cohomology ring for the Frobenius kernels G_d, $d \geq 2$. The previous authors already observed that the natural representation of a classical group has the above property (with no restriction on p). Our methods apply to any Chevalley group and hence give the result also for quasisimple groups with "exceptional type" root systems. The methods give explicit sufficient conditions on p; for an adjoint semisimple G with Coxeter number h, the condition $p > 2h - 2$ is always good enough.

1. INTRODUCTION

Let k be an algebraically closed field of characteristic $p > 0$, and let G be a connected, reductive group over k. We consider in this paper two questions which involve the relationship between nilpotent elements in the Lie algebra $\mathfrak{g}$ of G and certain unipotent subgroups of G.

1.1. There are finitely many (adjoint) orbits of G on the nilpotent elements of its Lie algebra $\mathfrak{g}$; since $\mathfrak{g}$ is a p-Lie algebra it is reasonable to ask for each nilpotent class $\mathrm{Ad}(G)X \subset \mathfrak{g}$ what is the minimal integer $m \geq 1$ for which $X^{[p^m]} = 0$.

The analogous question for unipotent elements in G was answered in [Tes95]; D. Testerman gave there a formula for the orders of the unipotent elements in G. We show here that the answer in both cases is "the same" and that moreover by first proving the Lie algebra result, one obtains a proof of Testerman's formula which avoids the calculations with explicit representatives for the unipotent classes that were carried out in *loc. cit.*

More precisely, we prove the following:

Theorem. *Assume that p is a good prime for the connected reductive group G, and that P is a distinguished parabolic subgroup of G with unipotent radical* V*. Write $n(P)$ for the nilpotence class of* V *(which is the same as the nilpotence class of $\mathfrak{v}$), and let the integer $m > 0$ be minimal with the property that $p^m \geq n(P)$.*

Date: March 16, 2001.

This work was supported by a grant from the National Science Foundation.

(1) *The p-nilpotence degree of a Richardson element of $\mathfrak{v} = \mathrm{Lie}(\mathrm{V})$ is m; equivalently, the p-exponent of the Lie algebra $\mathfrak{v}$ is m;*
(2) *The order of a Richardson element of V is p^m; equivalently, the exponent of V is p^m.*

In section 2 we recall general notions and definitions concerning nilpotent group and nilpotent Lie algebras. There is a simple formula for the nilpotence class $n(P)$ given in section 4.4. For m as in the theorem, it follows from generalities (see Lemma 2.1 and Proposition 4.4) that the p-nilpotence degree of X is $\leq m$ and that the order of u is $\leq p^m$. Thus, the theorem amounts to the following assertions: the exponent of V and the p-exponent of $\mathfrak{v}$ are as large as permitted by their respective nilpotence class.

In section 3, we discuss connected, Abelian, unipotent algebraic groups. In characteristic 0, any such group is a vector group, but that is not true in positive characteristic. On the other hand, in the positive characteristic case, any such group U is *isogenous* to a product of "Witt vector groups" whose dimensions are uniquely determined by U. Using this we observe that the p-exponent of $\mathrm{Lie}(U)$ is $\leq \log_p$ of the exponent of the group U; see Proposition 3.6.

In section 4, we review relevant facts concerning the classification of unipotent and nilpotent classes for reductive groups. The Bala-Carter theorem, as proved for all good primes p by Pommerening, parameterizes the nilpotent classes in the Lie algebra $\mathfrak{g}$ of G; thanks to a result of Springer, it then also parameterizes the unipotent classes in G.

If V is as in the theorem, a result of Spaltenstein shows that the centralizer dimension of a Richardson element $X \in \mathrm{Lie}(\mathrm{V})$ is "the same as in characteristic 0"; using this fact, we are able to use reduction modulo p arguments to obtain a lower bound on the nilpotence class of $\mathrm{ad}(X)$ which suffices for part (1) of the theorem; the details are contained in section 5.

Next, we locate a connected, Abelian, unipotent subgroup Z of G which meets the Richardson orbit of P on V, and moreover such that $\mathfrak{z} = \mathrm{Lie}(Z)$ meets the Richardson orbit of P on $\mathfrak{v}$. The results in section 3 show now that $\log_p$ of the exponent of Z must be $\geq$ the p-exponent of $\mathfrak{z}$, from which we deduce part (2) of the theorem. This argument is contained in section 6.

1.2. Let H denote a linear algebraic group over k defined over $\mathbb{F}_p$. In [SFB97a] and [SFB97b], Suslin, Friedlander, and Bendel relate the cohomology of the Frobenius kernel H_d to a certain affine scheme $\underline{\mathcal{A}}(d, H)$ whose k-points coincide with the set of all group scheme homomorphisms $\mathbb{G}_{a,d} \to H$. In fact, they show that the spectrum of the even cohomology ring of H_d is homeomorphic to $\underline{\mathcal{A}}(d, H)$. Let $\mathcal{A}(d, H)$ be the variety corresponding to $\underline{\mathcal{A}}(d, H)$ [if A denotes the coordinate ring of the scheme, then the coordinate ring of the variety is $A' = A/\sqrt{0}$; in this case, the maximal ideals of A' identify with the above group scheme homomorphisms]. We observe that $\mathcal{A}(d, H)$ and $\underline{\mathcal{A}}(d, H)$ are homeomorphic, and in this paper we will only work with the variety.

In case H is the full linear group $\mathrm{GL}(V)$ of a k-vectorspace V, $\mathcal{A}(d, H)$ has a simple description as the variety of commuting d-tuples of p-nilpotent elements of $\mathfrak{h} = \mathfrak{gl}(V)$.

For general H, one may take a faithful representation (ρ, V) of H and it was observed in [SFB97a] that $\mathcal{A}(d, H)$ is a somewhat mysterious closed subvariety of $\mathcal{A}(d, \mathrm{GL}(V))$. If for each p-nilpotent $X \in \mathfrak{g}$ the exponential homomorphism $t \mapsto \exp(d\rho(tX))$ takes values in H, we say that (ρ, V) is an exponential-type representation. It is shown in *loc. cit.* that if H has an exponential-type representation, then $\mathcal{A}(d, H)$ may be identified with the variety $\mathcal{N}_p(d, \mathfrak{h})$ of commuting d-tuples of p-nilpotent elements in $\mathfrak{h}$.

We show in this paper that if G is semisimple and p is sufficiently large, then G has an exponential-type representation. We consider exponentials in section 7; the results on exponentials in Chevalley groups may be found in 7.4. As a by-product of some of our constructions, we obtain also a new proof, for classical groups, of a recent result of Proud [Pro] concerning Witt-vector subgroups containing unipotent elements; see Theorem 7.5.

When p does not divide the order of the "fundamental group" of G, we show that $\mathcal{A}(d, G)$ is isomorphic to $\mathcal{A}(d, G_{\mathrm{sc}})$ as G_{sc}-varieties, where G_{sc} is the simply connected covering group; in this sense, $\mathcal{A}(d, G)$ is independent of isogeny. However, it is not at all clear whether the property of having an exponential-type representation is independent of isogeny.

When G is a classical group, it was observed in [SFB97a] that its "natural" module V defines an exponential-type representation (in any characteristic); so long as p does not divide the order of the fundamental group, this shows that $\mathcal{A}(d, G') \simeq \mathcal{N}_p(d, \mathfrak{g})$ for any quasisimple, semisimple group G' with root system of type A, B, C or D.

For a general semisimple group G we show that if $p > 2h - 2$ (where h is the Coxeter number), the adjoint module is an exponential-type representation for the corresponding adjoint group (which is isogenous to G); since this inequality also guarantees that p doesn't divide the order of the fundamental group, we get $\mathcal{A}(d, G) \simeq \mathcal{N}_p(d, \mathfrak{g})$ with this condition on p.

If G is an exceptional group of type E_8, our techniques do no better than the bound $p > 2h - 2 = 58$. For the other exceptional groups, we improve this bound slightly; see 9.5.

Suppose that G has an exponential-type representation. As observed in [SFB97a, Remark 1.9], it is not clear whether the resulting isomorphism $\mathcal{N}_p(d, \mathfrak{g}) \to \mathcal{A}(d, G)$ is intrinsic, or depends on the choice of exponential-type representation. In an attempt to study this question, we consider in section 8 a related result due to Serre concerning exponentials: if P is a parabolic subgroup of a reductive group G, and p exceeds the nilpotence class $n(P)$ of the unipotent radical V of P, then there is a P-equivariant isomorphism $\mathfrak{v} \to \mathrm{V}$ of algebraic groups, where $\mathfrak{v} = \mathrm{Lie}(\mathrm{V})$ is regarded as an algebraic group via the Hausdorff formula. As a consequence, we observe in 9.6 that one gets an intrinsically defined morphism of P-varieties $\mathcal{N}(d, \mathfrak{v}) \to \mathcal{A}(d, \mathrm{V})$ which we prove is injective. We have not so far been able to decide whether this morphism should be an isomorphism of varieties, or even surjective.

1.3. Some notations and conventions. If Λ is any commutative ring, and V a finitely generated Λ-module, we denote by $\mathrm{Aut}_\Lambda(V)$ the linear automorphisms of V. We denote by $\mathrm{GL}(V)$ the *affine group scheme of finite type* with $\mathrm{GL}(V)(\Lambda') = \mathrm{Aut}_{\Lambda'}(V \otimes_\Lambda \Lambda')$ for each commutative Λ-algebra Λ'.

If $\Lambda = \mathrm{E}$ is a field, we mostly prefer to identify affine group schemes of finite type over E which are absolutely reduced with the corresponding linear algebraic groups over E. Thus a finite dimensional E-vector space V determines a linear algebraic group $\mathrm{GL}(V)$ over E; this is an E-form of $\mathrm{GL}(V \otimes_{\mathsf{E}} \overline{\mathsf{E}})$, where $\overline{\mathsf{E}}$ denotes an algebraic closure of E.

1.4. I would like to thank Århus University for its hospitality during the academic year 2000/1. Also, thanks to Jens Jantzen for a number of helpful comments on this manuscript.

2. Nilpotent endomorphisms, groups, and Lie algebras

If M is an Abelian group and ϕ is an nilpotent endomorphism of M, the nilpotence degree of ϕ is the least positive integer e such that $\phi^e = 0$.

A group M, respectively a Lie algebra M, is nilpotent provided that its descending central series $M = C^0M \supset C^1M \supset \cdots$ terminates in 1, respectively 0, after finitely many steps [recall that for $i \geq 1$, we have $C^iM = (M, C^{i-1}M)$ for a group M, respectively $C^iM = [M, C^{i-1}M]$ for a Lie algebra M]. If M is nilpotent, its nilpotence class is the least e for which C^eM is trivial.

Let k be an algebraically closed field, and let L be the Lie algebra of a linear algebraic k-group; there is then a well-defined notion of a nilpotent element of L. Suppose now that the characteristic of k, say p, is positive; then L is a p-Lie algebra. Evidently $X \in L$ is nilpotent if and only if $X^{[p^e]} = 0$ for some e [the map $X \mapsto X^{[p^e]}$ is the e-th iteration of the p-power map on L]. The p-nilpotence degree of a nilpotent $X \in L$ is the minimal e for which $X^{[p^e]} = 0$. The element X is said to be p-nilpotent if its p-nilpotence degree is 1 (i.e. if $X^{[p]} = 0$).

We have (see [Bor91, §3.1]) for all $X_1, X_2, \ldots, X_r \in L$:

$$(1) \qquad \left(\sum_{i=1}^{r} X_i\right)^{[p]} \equiv \sum_{i=1}^{r} X_i^{[p]} \pmod{C^pL}$$

If moreover L is a nilpotent Lie algebra, then each element $X \in L$ is nilpotent. Since L is a finite dimensional p-Lie algebra, the p-nilpotence degree of any X in L is bounded; call the p-exponent of L the maximum of the p-nilpotence degree of its elements.

2.1. We have the following general result bounding "exponent" in terms of "nilpotence class".

Lemma. (a) *Let L be a nilpotent Lie algebra with class e. Assume for each $i \geq 0$ that C^iL has a k-basis of p-nilpotent elements. Then $X^{[p^e]} = 0$ for all $X \in L$ (i.e. the p-exponent of L is $\leq e$).*

(b) *Let G be a nilpotent group with class e. Assume for each $i \geq 0$ that C^iG is generated by elements of order p. Then $x^{p^e} = 1$ for all $x \in G$ (i.e. the exponent of G is $\leq p^e$).*

Proof. Note first that for $X = G$ or $X = L$ we have $(*)$ $C^iC^jX \subset C^{ij}X$ for all $i, j \geq 0$. To see this, first note that $(**)$ $(C^iG, C^jG) \subset C^{i+j+1}G$ and $[C^iL, C^jL] \subset C^{i+j+1}L$. In the group case, $(**)$ follows from [Hal76, Cor. 10.3.5] (note that our C^iG coincides with $\Gamma_{i+1}G$ in *loc. cit.*). In the case of the Lie algebra L, $(**)$ follows from [Jac62, I.7, Prop. 5] (again, our C^iL coincides with L^{i+1} in *loc. cit.*).

One now proves $(*)$ by induction on i, the result of course being trivial for $i = 0$. We consider the Lie algebra case, the argument for a group is the same.

Suppose that $i \geq 1$; using the induction hypothesis and $(**)$ one finds $C^iC^jL = [C^jL, C^{i-1}C^jL] \subset [C^jL, C^{j(i-1)}L] \subset C^{j+j(i-1)+1}L = C^{ij+1}L \subset C^{ij}L$.

To prove (a), let $X \in L$ and write $X = \sum_{i=1}^r X_i$ where $X_i^{[p]} = 0$ for all i. Then $X^{[p]} \in C^pL$ by (1). By $(*)$ we have $C^{p^{e-1}}C^pL \subset C^{p^e}L$ which is 0 by assumption. Thus by induction on e we find that $X^{[p^e]} = (X^{[p]})^{[p^{e-1}]} = 0$. The proof of (b) is essentially the same. □

3. Abelian unipotent groups

In this section, we recall some basic known facts about Abelian unipotent groups.

3.1. Witt vector groups. Let $p > 0$ be a prime number, let $n \geq 1$ be an integer, and let $W_{n,\mathbb{Z}_{(p)}}$ denote the group scheme over $\mathbb{Z}_{(p)}$ of the "Witt vectors of length n" for the prime p; see [Ser79, II.§6] and [Ser88, V.§16,VII.§7]. We write $W_n = W_{n,k}$ for the corresponding group over k.

Example. Let $F(X,Y) = \dfrac{X^p + Y^p - (X+Y)^p}{p} \in \mathbb{Z}[X,Y]$. When $n = 2$, the operation in $W_{2,\mathbb{Z}_{(p)}} = \mathbb{A}^2_{\mathbb{Z}_{(p)}}$ (here written additively) is defined by the rule

$$\vec{t} + \vec{s} = (t_0 + s_0, F(t_0, s_0) + t_1 + s_1).$$

More precisely, the co-multiplication for $\mathbb{Z}_{(p)}[W_n] = \mathbb{Z}_{(p)}[T_0, T_1]$ is given by

$$\Delta(T_0) = T_0 \otimes 1 + 1 \otimes T_0$$

and

$$\Delta(T_1) = T_1 \otimes 1 + 1 \otimes T_1 + F(T_0 \otimes 1, 1 \otimes T_0)$$

(1). *The underlying scheme of $W_{n,\mathbb{Z}_{(p)}}$ is isomorphic with the affine space ${\mathbb{A}^n}_{\mathbb{Z}_{(p)}}$, hence the structure algebra $\mathbb{Z}_{(p)}[W_n]$ is free over $\mathbb{Z}_{(p)}$.*

(2). *There is an isomorphism of $\mathbb{Q}$-group schemes*

$$\varphi : W_{n,\mathbb{Q}} \xrightarrow{\simeq} \mathbb{G}_{a,\mathbb{Q}} \times \cdots \times \mathbb{G}_{a,\mathbb{Q}} \quad \textit{(n factors).}$$

Proof. For $m \geq 1$, let

$$w_m = X_0^{p^m} + pX_1^{p^{m-1}} + \cdots + p^m X_m \in \mathbb{Z}[X_0, X_1, \dots].$$

We may define a map

$$\varphi : W_{n,\mathbb{Q}} \to \mathbb{G}_{a,\mathbb{Q}} \times \cdots \times \mathbb{G}_{a,\mathbb{Q}}$$

by assigning, for each $\mathbb{Q}$-algebra Λ and each $\vec{t} \in W_{n,\mathbb{Q}}(\Lambda)$, the value

$$\varphi(\vec{t}) = (w_0(\vec{t}), w_1(\vec{t}), \dots, w_{n-1}(\vec{t})).$$

Since p is invertible in $\mathbb{Q}$, it follows from [Ser79, Theorem II.6.7] that φ is an isomorphism of $\mathbb{Q}$-group schemes. [Note that the assertion is valid over any field F provided only that the characteristic of the field F is different from p.] □

3.2. The Artin-Hasse exponential series. Now let $F(t) \in \mathbb{Q}[\![t]\!]$ be the power series

$$F(t) = \exp(-(t + t^p/p + t^{p^2}/p^2 + \cdots)).$$

If μ denotes the Möbius function, one easily checks the identity of formal series

$$F(t) = \prod_{(m,p)=1, m\geq 1} (1 - t^m)^{\mu(m)/m},$$

by taking logarithms and using the fact that

$$\sum_{d|m} \mu(d) = 0$$

if $m \neq 1$. It then follows that *the coefficients of $F(t)$ are integers at p*; i.e. $F(t) \in \mathbb{Z}_{(p)}[\![t]\!]$.

3.3. If $\mathcal{L}$ is a $\mathbb{Z}_{(p)}$-lattice, and $X \in \operatorname{End}_{\mathbb{Z}_{(p)}}(\mathcal{L})$ is a nilpotent endomorphism such that $X^{p^n} = 0$, then there is a homomorphism of $\mathbb{Z}_{(p)}$-group schemes

$$E_X : W_{n,\mathbb{Z}_{(p)}} \to \mathrm{GL}(\mathcal{L})$$

given for each $\mathbb{Z}_{(p)}$-algebra Λ by $E_X(\vec{t}) = F(t_0X)F(t_1X^p)\cdots F(t_{n-1}X^{p^{n-1}})$ for $\vec{t} \in W_n(\Lambda)$; see [Ser88, V§16].

Let $V_\mathbb{Q} = \mathcal{L} \otimes_{\mathbb{Z}_{(p)}} \mathbb{Q}$. There are maps

$$E_X : W_{n,\mathbb{Q}} \to \mathrm{GL}(V_\mathbb{Q}) \quad \text{and} \quad E_{\overline{X}} : W_{n,\mathbb{F}_p} \to \mathrm{GL}(\mathcal{L}/p\mathcal{L}).$$

obtained by base change.

Lemma. (1) *Over $\mathbb{Q}$, E_X factors as*

$$\begin{tikzcd}
W_{n,\mathbb{Q}} \arrow[r, "E_X"] \arrow[dr, "\varphi"'] & \mathrm{GL}(V_\mathbb{Q}) \\
& \mathbb{G}_{a,\mathbb{Q}} \times \cdots \times \mathbb{G}_{a,\mathbb{Q}} \arrow[u, "\vec{s}\mapsto\exp(\sum_{j=0}^{n-1} p^{-j} s_j X^{p^j})"']
\end{tikzcd}$$

where φ is the isomorphism of 3.1(2).

(2) *The endomorphism $\overline{X}$ of $\mathcal{L}/p\mathcal{L}$ is in the image of the Lie algebra homomorphism*

$$dE_{\overline{X}} : \mathfrak{w}_{n,\mathbb{F}_p} \to \mathfrak{gl}(\mathcal{L}/p\mathcal{L}).$$

Proof. For each $\mathbb{Q}$-algebra Λ and each $\vec{t} \in W_n(\Lambda)$ one uses induction on n and the definition of the w_j to verify that

$$\sum_{j=0}^{n-1} p^{-j} w_j(\vec{t}) X^{p^j} = \sum_{m=0}^{n-1} \sum_{l=0}^{n-1-m} p^{-l} (t_m X^{p^m})^{p^l}.$$

It follows that

$$\exp\left(\sum_{j=0}^{n-1} p^{-j} w_j(\vec{t}) X^{p^j}\right) = \prod_{m=0}^{n-1} F(t_m X^{p^m}) = E_X(\vec{t}),$$

whence (1).

For (2), let $T_0, \ldots, T_{n-1}$ denote the coordinate functions on $W_{n,\mathbb{F}_p}$ with $T_i(\vec{t}) = t_i$; thus $A = \mathbb{F}_p[W_n]$ is a polynomial ring in the T_i. The tangent space to W_n at 0 contains the “point-derivation” $D : A \to \mathbb{F}_p$ given by $f \mapsto \dfrac{\partial f}{\partial T_0} \mid_{\vec{t}=0}$, and it is clear that $dE_{\overline{X}}(D) = \overline{X}$. □

3.4. The Lie algebra of the Witt vectors. Let V be a k-vector space of dimension $p^{n-1}+1$, and let $X \in \mathrm{End}_k(V)$ be a nilpotent “Jordan block” of size $p^{n-1}+1$. Thus $X^{p^{n-1}} \neq 0$ while $X^{p^n} = 0$. The smallest p-Lie subalgebra of $\mathfrak{gl}(V)$ containing X is then the Abelian Lie algebra $\mathfrak{a} = \sum_{i=0}^{n-1} kX^{p^i} = \sum_{i=0}^{n-1} kX^{[p^i]}$.

Let $E_X : W_n \to \mathrm{GL}(V)$ be the homomorphism determined by X as in 3.3.

Proposition. *If k is a field of characteristic p, then $\mathfrak{w}_n = \mathrm{Lie}(W_n)$ is an Abelian Lie algebra with a k-basis $Z_0, Z_1, \dots, Z_{n-1}$ such that $Z_i = Z_0^{[p^i]}$ for $0 \leq i \leq n-1$.*

Proof. Let $\mathfrak{b}$ be the image of dE_X; thus $\mathfrak{b}$ is a p-Lie subalgebra of $\mathfrak{gl}(V)$. According to Lemma 3.3, $\mathfrak{b}$ contains X. It follows that $\mathfrak{a} \subset \mathfrak{b}$. On the other hand, we have

$$n = \dim_k \mathfrak{a} \leq \dim_k \mathfrak{b} \leq \dim W_{n,k} = n.$$

Thus $\mathfrak{a} = \mathfrak{b} \simeq \mathfrak{w}_n$, and the proposition follows. □

Example. Say $n = 2$. Then $k[W_2] = k[T_0, T_1]$. One can show that $X_0 = \dfrac{\partial}{\partial T_0} + T_0^{p-1}\dfrac{\partial}{\partial T_1}$ and $X_1 = \dfrac{\partial}{\partial T_1}$ are W_2-invariant derivations of $k[W_2]$, and that these derivations span $\mathfrak{w}_2$. A simple computation yields $X_0^{[p]} = X_1$.

3.5. Exponents.

Proposition. (1) *The p-exponent of $\mathfrak{w}_n = \mathrm{Lie}(W_n)$ is n.*

(2) *The exponent of W_n is p^n; moreover, a Witt vector $\vec{t} \in W_n(k)$ has order p^n if and only if $t_0 \neq 0$.*

Proof. Part (1) follows immediately from the description of $\mathfrak{w}_n$ given by Proposition 3.4. For (2), recall [Ser79, Theorem II.6.8] that the ring of (infinite) Witt vectors $W(k)$ is a strict p-ring (see *loc. cit.* II.5 for the definition) and that $W_m(k) \simeq W(k)/p^m W(k)$ for all $m \geq 1$. (2) now follows at once. □

3.6. Connected Abelian unipotent groups. Recall that two connected Abelian algebraic groups G and H are said to be *isogenous* if there is a surjection $G \to H$ whose kernel is finite.

Lemma. *If G and H are connected Abelian algebraic groups which are isogenous, then the exponent of G is equal to the exponent of H.*

Proof. The lemma is clear if either G or H has infinite exponent, so assume otherwise. Suppose that $\phi : G \to H$ is a surjection with finite kernel. Let m be the exponent of H. Since G is Abelian, the map $x \mapsto x^m$ defines a group homomorphism $G \to \ker \phi$; since G is connected and $\ker \phi$ is finite, this homomorphism must be trivial. It follows that $x^m = 1$ for all $x \in G$, and this shows that the exponent of G is $\leq$ that of H. The inequality $\geq$ is immediate since ϕ is surjective. □

Proposition. *Let U be a connected Abelian unipotent group over k. Then*

(1) *U is isogenous to a product of Witt groups $\prod_{i=1}^{d} W_{n_i,k}$; moreover, the integers n_i are uniquely determined (up to order) by U.*

Let $n = \max_i(n_i)$ where the n_i are as in 1.

(1) *The exponent of the group U is p^n.*
(2) *The p-exponent of $\mathfrak{u} = \operatorname{Lie}(U)$ is $\leq n$.*

Proof. The first assertion is [Ser88, VII§2 Theorem 1]. The second assertion follows immediately from the lemma.

For the last assertion, it is proved in [Ser88, VII§2 Theorem 2] that the group U is a *subgroup* of a product of Witt groups. A careful look at the proof in *loc. cit.* shows that the exponent of U and this product may be chosen to coincide. Thus, $\mathfrak{u}$ is a subalgebra of $\mathfrak{w}$, a product of Lie algebras $\mathfrak{w}_{n_i}$ with $\max(p^{n_i})$ equal to the exponent of U; (3) now follows since the p-exponent of the Lie subalgebra $\mathfrak{u}$ can't exceed that of $\mathfrak{w}$. □

Remark. The p-exponent of $\operatorname{Lie}(U)$ may indeed be strictly smaller than $\log_p$ of the exponent of U. Let V_2 be the algebraic k-group which is isomorphic as a variety to $\mathbb{A}^2_k$, with the group operation in V_2 determined by

$$\vec{t} + \vec{s} = (t_0 + s_0, F(t_0, s_0)^p + t_1 + s_1).$$

Then the map $\varphi : W_2 \to \mathrm{V}_2$ given by $\vec{t} \mapsto (t_0^p, t_1)$ is a (purely inseparable) isogeny. The exponent of V_2 is p^2, but every element $x \in \mathfrak{v}_2 = \operatorname{Lie}(\mathrm{V}_2)$ satisfies $x^{[p]} = 0$. Indeed, one can check that $\dfrac{\partial}{\partial T_0}$ and $\dfrac{\partial}{\partial T_1}$ are V_2-invariant derivations of $k[\mathrm{V}_2]$, and that they span $\mathfrak{v}_2$ over k.

4. Reductive groups

4.1. Generalities. Let G be a connected reductive group over the field k which is defined and split over the prime field $\mathbb{F}_p$. We fix a maximal torus T contained in a Borel subgroup B of G. Let $X = X^*(T)$ be the group of characters of T, and $Y = X_*(T)$ be the group of co-characters. The adjoint action of G on its Lie algebra $\mathfrak{g}$ is diagonalizable for T; the non-zero weights of this action form a root system $R \subset X$, and the choice of Borel subgroup determines a system of positive roots R^+ and a system of simple roots S. Write $\langle ?, ? \rangle$ for the canonical pairing $X \times Y \to \mathbb{Z}$.

For each root $\alpha \in R^+$, there is a root homomorphism $\phi_\alpha : \mathbb{G}_a \to U$; the product (in any fixed order) of the root homomorphisms ϕ_α with $\alpha > 0$ defines an isomorphism of varieties $\mathbb{A}^{|R^+|} \to U$.

For each $\alpha \in R^+$ the derivative of ϕ_α yields an element $e_\alpha \in \mathfrak{u} = \operatorname{Lie}(U)$; the e_α form a basis for $\mathfrak{u}$.

4.2. Good primes. We will usually assume that p is a good prime for G. If the root system of G is indecomposable, let β be the short root of maximal height. In that case, the prime p is good for G provided that if $\beta^\vee = \sum_{\alpha \in S} a_\alpha \alpha^\vee$, then all a_α are prime to p. For indecomposable root systems, p is bad (=not good) just in case one of the following holds: $p = 2$ and R is not of type A_r; $p = 3$ and R is of type G_2, F_4 or E_r; or $p = 5$ and R is of type E_8. In general p is good for G if it is good for each indecomposable component of the root system R.

4.3. Parabolic subgroups. Let P be a parabolic subgroup of G containing the Borel subgroup B, and let $\mathfrak{p}$ be the Lie algebra of P. Put $I = \{\alpha \in S \mid \mathfrak{p}_{-\alpha} \neq 0\}$. The parabolic subgroup P is then

$$P = \langle B, \operatorname{Im} \phi_{-\alpha} \mid \alpha \in I \rangle.$$

The group P has a Levi decomposition $P = \mathrm{L}\mathrm{V}$ where L is a reductive group and V is the unipotent radical of P. The derived group of the Levi factor L is a semisimple group whose root system R_P is generated by the roots in I. Denote by $\mathfrak{v} = \mathrm{Lie}(\mathrm{V})$ the nilradical of $\mathfrak{p}$. As a variety, the group V is the product of the images of the root homomorphism ϕ_α with $\alpha \in R^+ \setminus R_P$.

There is (see e.g. [Spr98, Ch. 9]) an isogeny

$$\hat{G} = \prod_i G_i \times T \to G$$

where each G_i is semisimple with indecomposable root system, and T is a torus. Let $\hat{P}$ denote the parabolic subgroup of $\hat{G}$ determined by I, and let $\hat{\mathrm{V}}$ denote its unipotent radical.

Lemma. *The above isogeny restricts to an isomorphism $\hat{\mathrm{V}} \simeq \mathrm{V}$; moreover, we have $\hat{\mathrm{V}} \simeq \prod_i \hat{\mathrm{V}}_i$ where $\hat{\mathrm{V}}_i = \mathrm{V} \cap G_i$.*

Proof. This follows from [Bor91, Prop. 22.4]. □

4.4. Associated with the parabolic subgroup P, we may define a homomorphism $f : \mathbb{Z}R \to \mathbb{Z}$ given by

$$f(\alpha) = \begin{cases} 0 & \text{if } \alpha \in S \text{ and } -\alpha \in R_P \\ 2 & \text{if } \alpha \in S \text{ and } -\alpha \notin R_P \end{cases}$$

Such a homomorphism induces a grading of the Lie algebra $\mathfrak{g} = \bigoplus_{i\in\mathbb{Z}} \mathfrak{g}(i)$ by setting $\mathfrak{g}(i) = \bigoplus_{f(\alpha)=i} \mathfrak{g}_\alpha$. We have evidently $\mathrm{Lie}(P) = \mathfrak{p} = \bigoplus_{i\geq 0} \mathfrak{g}(i)$ and $\mathrm{Lie}(\mathrm{V}) = \mathfrak{v} = \sum_{i>0} \mathfrak{g}(i)$. We have by construction that

$$\mathfrak{g}(i) \neq 0 \implies i \equiv 0 \pmod 2.$$

When R is indecomposable, let $\tilde{\alpha} \in R^+$ be the long root of maximal height, and let $n(P) = \frac{1}{2}f(\tilde{\alpha}) + 1$. If we write $\tilde{\alpha}$ as a $\mathbb{Z}$-linear combination of the simple roots S, then $n(P) - 1$ is just the sum of the coefficients in this expression of the roots in $S \setminus I$.

Note that

$$\mathfrak{g}(i) \neq 0 \implies -f(\tilde{\alpha}) \leq i \leq f(\tilde{\alpha})$$

and that $\mathrm{Lie}(T) \subset \mathfrak{g}(0) \neq 0$ and $e_{\tilde{\alpha}} \in \mathfrak{g}(f(\tilde{\alpha})) \neq 0$.

When R is no longer indecomposable, let S' be the simple roots for an indecomposable component R' of R, and let $\tilde{\alpha}'$ be the highest long root in R'. Put $n(P, S') = \dfrac{1}{2}f(\tilde{\alpha}') + 1$, and let $n(P)$ be the supremum of the $n(P, S')$.

Proposition. *Suppose that p is a good prime for G, let P be a distinguished parabolic subgroup, and let $m \geq 1$ be minimal with $p^m \geq n(P)$.*

(a) *The nilpotence class of the Lie algebra $\mathfrak{v}$ is $n(P)$.*
(b) *The p-exponent of $\mathfrak{v}$ is $\leq m$.*
(c) *The nilpotence class of the group V is $n(P)$.*
(d) *The exponent of V is $\leq p^m$.*

Proof. We first prove (a) and (c). By Lemma 4.3, we are reduced to the case where R is indecomposable.

Since p is good, [BT73, Prop. 4.7] shows that $C^{j-1}\mathrm{V} = \prod_{f(\alpha)\geq 2j} \operatorname{Im}\phi_\alpha$ for $j \geq 1$. Essentially the same arguments show that $C^{j-1}\mathfrak{v} = \sum_{f(\alpha)\geq 2j} ke_\alpha$. Since every root α satisfies $f(\tilde{\alpha}) \geq f(\alpha)$; (a) and (c) now follow at once.

Note that we have showed for all $i \geq 0$ that $C^i\mathfrak{v}$ has a basis of p-nilpotent vectors (the root vectors) and that $C^i\mathrm{V}$ is generated by elements of order p (the images of root homomorphisms). By Lemma 2, (b) now follows from (a), and (d) follows from (c). □

Corollary. *If $p \geq h$, every nilpotent element $Y \in \mathfrak{g}$ satisfies $Y^{[p]} = 0$ and every unipotent element $1 \neq u \in G$ has order p.*

Proof. Let Y be a *regular nilpotent* element in $\mathfrak{u} = \operatorname{Lie}(U)$; thus Y is a representative for the dense B-orbit on $\mathfrak{u}$ [see the discussion of Richardson's dense orbit theorem below in section 4.5]. Since $n(B) = h$, the proposition shows that $Y^{[p]} = 0$. Since the regular nilpotent elements form a single dense orbit in the nilpotent variety, we get $Y^{[p]} = 0$ for every nilpotent Y. The assertion for unipotent elements follows in the same way. □

Remarks. (1) Suppose that G is semisimple; thus S is a $\mathbb{Q}$ basis for $X_\mathbb{Q}$. Then f determines, by extension of scalars, a unique $\mathbb{Q}$-linear map $f_\mathbb{Q} : X_\mathbb{Q} \to \mathbb{Q}$. For some $q \in \mathbb{Z}$, the homomorphism $qf_\mathbb{Q}$ maps X to $\mathbb{Z}$, so that $qf = \phi \in Y$, the group of cocharacters of the maximal torus T. [In fact, this is true even when G is only assumed to be reductive, rather than semisimple.] For any such integer q, we have $\mathfrak{g}(i) = \{Y \in \mathfrak{g} \mid \operatorname{Ad}(\phi(t))Y = t^{qi}Y\}$, which makes it clear that the grading of $\mathfrak{g}$ is a grading as a p-Lie algebra. In particular, if $Y \in \mathfrak{g}(i)$, we have $Y^{[p]} \in \mathfrak{g}(pi)$.

(2) The preceding remark permits an alternate proof of (b) of the proposition; indeed, for a homogeneous $Y \in \mathfrak{v}(i)$ [so $i > 0$], we have $Y^{[p^m]} \in \mathfrak{g}(p^m i) = 0$.

(3) The corollary is of course well known; I didn't find a suitable reference, however. Jens Jantzen has pointed out to me a somewhat more elementary argument that $X^{[p]} = 0$ for $X \in \mathfrak{g}$ nilpotent when $p \geq h$. We may assume X to be in $\mathfrak{u}$; thus we may write $X = \sum_{\alpha\in R^+} a_\alpha e_\alpha$ with scalars $a_\alpha \in k$. By Jacobson's formula for the p-th power of a sum, $X^{[p]}$ is $\sum_{\alpha\in R^+} a_\alpha^p e_\alpha^{[p]} + L$ where L is a linear combination of commutators of length p. Now, all summands of L are weight vectors of a weight that has height $\geq p$. But the maximal height of a root is $h - 1 < p$.

4.5. The Bala-Carter parameterization of nilpotent elements. Let G be connected and reductive in good characteristic p, and let $P = \mathrm{LV}$ be a parabolic subgroup. The adjoint action P on $\mathfrak{g}$ leaves $\mathfrak{v}$ invariant. A theorem of Richardson [Hum95, Theorem 5.3] guarantees that P has a unique open orbit on $\mathfrak{v}$, and a unique open orbit on V; these are the Richardson orbits of P, and representatives for these orbits are called Richardson elements.

A nilpotent element $X \in \mathfrak{g}$ is *distinguished* if the connected center of G is a maximal torus of $C_G(x)$. [If G is semisimple, this means that any semisimple element of $C_G(x)$ is central].

On the other hand, the parabolic subgroup P is called *distinguished* if

$$\dim \mathfrak{g}(0) - \dim Z(G) = \dim \mathfrak{g}(2).$$

[Note that this differs from the definition in [Car93, p.167], but that Corollary 5.8.3 of *loc. cit.* shows that it is equivalent in case p is good.]

The following relates these two notions of distinguished:

Proposition. [Car93, Prop. 5.8.7] *If P is distinguished, then a Richardson element in $\mathfrak{v}$ is a distinguished nilpotent element. Moreover, the Richardson orbit on $\mathfrak{v}$ meets $\mathfrak{g}(2)$ in an open* L*-orbit.*

The full Bala-Carter theorem is as follows:

Proposition. Bala,Carter [BC76a, BC76b], Pommerening [Pom77, Pom80] *There is a bijection between the G-orbits of nilpotent elements in $\mathfrak{g}$ and the conjugacy classes of pairs (L, Q) where L is a Levi subgroup of a parabolic subgroup of G, and Q is a distinguished parabolic subgroup of L. The nilpotent orbit determined by (L, Q) is the one meeting the nilradical of* $\operatorname{Lie}(Q)$ *in its Richardson orbit.*

5. THE p-EXPONENT OF $\mathfrak{v}$

Throughout this section and the next, G is a reductive group, P is a distinguished parabolic subgroup with Levi decomposition $P = \mathsf{L}\mathsf{V}$. The characteristic p is assumed to be good for G.

5.1. Let A be a discrete valuation ring, with residue field of characteristic p and quotient field F. We assume chosen some fixed embedding of the residue field of A in our algebraically closed field k.

If $\mathcal{L}$ is an A-lattice and ψ is a nilpotent A-endomorphism, one might hope to relate the Jordan block structure of ψ_k and ψ_F [If $\psi \in \operatorname{End}_A(\mathcal{L})$, the corresponding endomorphisms of $L_\mathsf{F} = \mathcal{L} \otimes_A \mathsf{F}$ and L_k will be denoted ψ_F and ψ_k]. Since the dimension of the kernel of a liner transformation is equal to the number of its Jordan blocks, one must require that $\dim_k \ker \psi_k = \dim_\mathsf{F} \ker \psi_\mathsf{F}$. However, even with that condition, the partitions can be different; indeed, let π be a prime element of A and consider the endomorphism ψ of the lattice $A^4 = \bigoplus_{i=1}^4 Ae_i$ determined by the rules $\psi(e_1) = 0$, $\psi(e_2) = \psi(e_3) = e_1$, $\psi(e_4) = (\pi - 1)e_2 + e_3$. Then ψ_F has partition $(3, 1)$ while ψ_k has partition $(2, 2)$.

On the other hand, one has the following straightforward result. Let $\mathcal{L}$ be an A-lattice which is $2\mathbb{Z}$-graded; say

$$\mathcal{L} = \bigoplus_{i=0}^{d} \mathcal{L}_{2i}, \quad \mathcal{L}_0 \neq 0, \quad \mathcal{L}_{2d} \neq 0.$$

Let $\mathcal{L}^+ = \bigoplus_{i>0} \mathcal{L}_{2i}$, L_F^+ and L_k^+ be in each case the sum of the homogeneous components of positive degree.

Proposition. *Suppose $\psi \in \operatorname{End}_A(\mathcal{L})$ is an endomorphism of degree 2 (i.e. $\psi(\mathcal{L}_i) \subset \mathcal{L}_{i+2}$ for all i), and assume $\psi_\mathsf{F} : L_\mathsf{F} \to L_\mathsf{F}^+$ is surjective, so that the nilpotence degree of ψ is $d + 1$. If $\dim_k \ker \psi_k = \dim_\mathsf{F} \ker \psi_\mathsf{F}$, then $\psi : \mathcal{L} \to \mathcal{L}^+$ is surjective. In particular, $\psi_k^d \neq 0$, hence the nilpotence degree of ψ_k is also $d + 1$.*

Proof. It suffices to show that $\psi_k : L_k \to L_k^+$ is surjective. Since $\dim_\mathsf{F} L_\mathsf{F} = \dim_k L_k$ and $\dim_\mathsf{F} L_\mathsf{F}^+ = \dim_k L_k^+$, that follows immediately from the assumption on kernel dimensions. □

5.2. Let $G_{\mathbb{Z}}$ be a split reductive group scheme over $\mathbb{Z}$ which gives rise to G upon base change. There is a general notion of the Lie algebra $\mathfrak{g}_{\mathbb{Z}}$ of the affine group scheme $G_{\mathbb{Z}}$; see [Jan87, I.7.7]. In the case of our split reductive group, $\mathfrak{g}_{\mathbb{Z}}$ may be described explicitly; see [Jan87, II.1.11]. For any commutative ring A, let $\mathfrak{g}_A = \mathfrak{g}_{\mathbb{Z}} \otimes_{\mathbb{Z}} A$. The explicit description of $\mathfrak{g}_{\mathbb{Z}}$ implies that it is a $\mathbb{Z}$-lattice in the split reductive $\mathbb{Q}$-Lie algebra $\mathfrak{g}_{\mathbb{Q}}$, and that $\mathrm{Lie}(G) = \mathfrak{g} = \mathfrak{g}_k$. If $X_{\mathbb{Z}} \in \mathfrak{g}_{\mathbb{Z}}$, denote by X_A the element $X_{\mathbb{Z}} \otimes 1 \in \mathfrak{g}_A$.

Let P be a distinguished parabolic subgroup P, and let the map $f : \mathbb{Z}R \to \mathbb{Z}$ be as in 4.4; then f induces also a grading of $\mathfrak{g}_{\mathbb{Z}}$ (this again relies on the explicit description of $\mathfrak{g}_{\mathbb{Z}}$ mentioned above).

Fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$.

Lemma. *There is a finite subextension $\mathbb{Q} \subset \mathsf{F} \subset \overline{\mathbb{Q}}$ and a valuation ring $A \subset \mathsf{F}$, whose residue field we embed in k, such that the following holds: for some $X_A \in \mathfrak{g}_A(2)$, the element X_k is Richardson in $\mathfrak{v}$, and X_{F} is Richardson in $\mathfrak{v}_{\overline{\mathbb{Q}}}$.*

[This lemma is implicit in [Spa84]; we include a proof for the convenience of the reader.]

Proof. The Richardson orbit on $\mathfrak{v}_{\bar{\mathbb{Q}}}$ meets $\mathfrak{g}_{\bar{\mathbb{Q}}}(2)$ in an open set, so we may find a regular function f on $\mathfrak{g}_{\bar{\mathbb{Q}}}(2)$ such that $f(Y) \neq 0$ implies Y is a Richardson element. Using the lattice $\mathfrak{g}_{\mathbb{Z}}(2)$ in $\mathfrak{g}_{\bar{\mathbb{Q}}}(2)$, we obtain coordinate functions [dual to the root-vector basis] on $\mathfrak{g}_{\bar{\mathbb{Q}}}(2)$; let $\mathsf{F} \subset \bar{\mathbb{Q}}$ by a finite extension of $\mathbb{Q}$ containing the coefficients of f with respect to these coordinate functions. Take for A the localization of the ring of integers of F at some prime lying over (p), and fix some embedding of the residue field of A in k. If π denotes a prime element of A, we may multiply f be a suitable power of π and assume that all the coefficients of f are in A, and that not all are 0 modulo π. Let $\hat{f} \in k[\mathfrak{g}(2)]$ be the function obtained by reducing f modulo π. Then the distinguished open set determined by $\hat{f}$ is non-empty and so must meet the set of Richardson elements in $\mathfrak{g}(2)$. After possibly enlarging F and A, we may suppose that there is a Richardson element $X \in \mathfrak{g}(2)$ with $\hat{f}(X) \neq 0$, and such that the coefficients of X (in the root-vector basis) lie in the residue field of A. It is then clear that any lift X_A of X to $\mathfrak{g}_A(2)$ has the desired property. □

The main result obtained by Spaltenstein in [Spa84] implies the following:

Proposition. *Assume that the root system of G is indecomposable, and moreover that p is a good prime if R is not of type A_r, and that $G = \mathrm{GL}_{r+1}$ if $R = A_r$. Choose a finite extension F of $\mathbb{Q}$ with ring of integers A as in the lemma; let $X_A \in \mathfrak{v}_A$ be such that $X = X_k$ is a Richardson element of $\mathfrak{v}$ and X_{F} is a Richardson element of $\mathfrak{v}_{\mathsf{F}}$. Then*

(1) $\mathfrak{c}_{\mathfrak{g}}(X) \subset \mathfrak{p}$, *and*
(2) $\dim_{\mathsf{F}} \mathfrak{c}_{\mathfrak{g}_{\mathsf{F}}}(X_{\mathsf{F}}) = \dim_k \mathfrak{c}_{\mathfrak{g}}(X)$.

Remark. This result was also obtained by Premet in [Pre95].

5.3. Let F be a field of characteristic 0, and let $\mathfrak{sl}_2(\mathsf{F})$ be the split simple Lie algebra over F of 2×2 matrices with trace 0. This Lie algebra has an F-basis X, Y, H, where $[H, X] = 2X$, $[H, Y] = -2Y$, and $[X, Y] = H$. The semisimple element H acts diagonally on any finite dimensional representation (ρ, M), and the weights of H (=eigenvalues of $\rho(H)$) on M are integers. Write M_i for the i-th weight space.

The following is an easy consequence of the classification of finite dimensional representations for $\mathfrak{sl}_2(\mathsf{F})$:

Lemma. *Let (ρ, M) be a finite dimensional $\mathfrak{sl}_2(\mathsf{F})$-module such that all eigenvalues of $\rho(H)$ on M are even. Then $\rho(X) : \bigoplus_{i \geq 0} M_i \to \bigoplus_{i>0} M_i$ is surjective.*

5.4. We can now prove the statement of theorem 1.1 for the Lie algebra.

Theorem. (p-exponent formula) *Let $m \geq 1$ be the minimal integer with $p^m \geq n(P)$. Then the p-exponent of $\mathfrak{v}$ is m, and the p-nilpotence degree of a Richardson element of $\mathfrak{v}$ is m.*

Proof. In view of Lemma 4.3, we may suppose that G satisfies the hypothesis of Proposition 5.2.

With m as in the statement of the theorem, Proposition 4.4 shows that the p-nilpotence degree of any element of $\mathfrak{v}$ is $\leq m$; to prove that equality holds, it suffices to exhibit a representation (ρ, W) of $\mathfrak{p}$ as a p-Lie algebra in which some $\rho(X)^{n(P)-1}$ acts non-trivially. Take $(\rho, W) = (\mathrm{ad}, \mathfrak{p})$; we show that $\mathrm{ad}(X)^{n(P)-1} \neq 0$ for a suitable (and hence any) Richardson element.

First, use the lemma to find a finite extension F of $\mathbb{Q}$, a valuation ring $A \subset \mathsf{F}$, and an element $X_A \in \mathfrak{g}_A(2)$ such that $X = X_k \in \mathfrak{v}$ is Richardson, and $X_{\mathsf{F}} \in \mathfrak{v}_{\overline{\mathbb{Q}}}$ is Richardson.

The discussion in 4.4 shows that the lattice $\mathfrak{p}_A$ is $2\mathbb{Z}$ graded as in 5.1 with $d = n(P) - 1$. In the notation of Lemma 5.1, we have $L_{\mathsf{F}} = \mathfrak{p}_{\mathsf{F}}$ and $L_{\mathsf{F}}^+ = \mathfrak{v}_{\mathsf{F}}$. Note that $\mathrm{ad}(X_A) : \mathfrak{p}_A \to \mathfrak{p}_A$ has degree 2.

It follows from [Car93, Prop. 5.8.8] (or more precisely, the proof of that Proposition) that there are elements $Y, H \in \mathfrak{g}_{\overline{\mathbb{Q}}}$ such that H is semisimple, $\overline{\mathbb{Q}}Y + \overline{\mathbb{Q}}H + \overline{\mathbb{Q}}X_{\mathsf{F}}$ is a subalgebra isomorphic to $\mathfrak{sl}_2$, and such that the grading of $\mathfrak{g}_{\overline{\mathbb{Q}}}$ determined by H is the same as that determined by the function f as in 4.4. Thus for each $i \in \mathbb{Z}$ we have $\mathfrak{g}_{\overline{\mathbb{Q}}}(i) = \{Z \in \mathfrak{g}_{\overline{\mathbb{Q}}} \mid [H, Z] = iZ\}$. Applying Lemma 5.3 we see that $\mathrm{ad}(X_{\mathsf{F}}) : \mathfrak{p}_{\overline{\mathbb{Q}}} \to \mathfrak{v}_{\overline{\mathbb{Q}}}$ is surjective, from which it follows that $\mathrm{ad}(X_{\mathsf{F}}) : \mathfrak{p}_{\mathsf{F}} \to \mathfrak{v}_{\mathsf{F}}$ is surjective.

Proposition 5.2(1) shows that $\dim_k \mathfrak{c}_{\mathfrak{p}}(X) = \dim_k \mathfrak{c}_{\mathfrak{g}}(X)$. If we regard $\mathrm{ad}(X_{\mathsf{F}})$ and $\mathrm{ad}(X)$ as endomorphisms respectively of $\mathfrak{p}_{\mathsf{F}}$ and of $\mathfrak{p}$, then (2) of that proposition yields $\dim_{\mathsf{F}} \ker \mathrm{ad}(X_{\mathsf{F}}) = \dim_k \ker \mathrm{ad}(X)$; thus we apply Lemma 5.1 to conclude that $\mathrm{ad}(X)^{n(P)-1}(\mathfrak{p}) \neq 0$ as desired. □

6. THE EXPONENT OF V

Recall that we have fixed G a reductive group in good characteristic, and P a distinguished parabolic subgroup with Levi decomposition $P = \mathrm{LV}$.

6.1. A Theorem of Springer. We recall the following important result.

Proposition. *Let G be quasisimple, and assume that p is a good prime for G. If the root system is of type A, assume that the isogeny $G_{\mathrm{sc}} \to G$ is separable. Then there is a B-equivariant isomorphism of varieties $\varepsilon : \mathfrak{u} \to U$ which extends to a G-equivariant isomorphism of varieties ε between the nilpotent variety of $\mathfrak{g}$ and the unipotent variety of G.*

A version of the proposition was first proved by Springer [Spr69], though with the slightly weaker conclusion that ε is a homeomorphism. We refer the reader to the discussion of this result in [Hum95, 6.20/1].

In view of the equivariance property, it is clear that ε restricts to a P-isomorphism $\mathfrak{v} \to \mathrm{V}$, where $\mathfrak{v} \subset \mathfrak{u}$ is the Lie algebra of V. If $X \in \mathfrak{v}$ is a Richardson element, we let $R(X)$ denote the unipotent radical of the centralizer of X in G; note that $R(X)$ coincides with the centralizer in V of X.

Corollary. *Assume that G satisfies the hypothesis of the proposition, and let $X \in \mathfrak{v}$ be a Richardson nilpotent element.*

1. *Let Z be the center of $R(X)$. Then Z is a connected group, and X is tangent to Z; i.e. $X \in \mathrm{Lie}(Z)$.*
2. *The exponent of the connected, Abelian, unipotent group Z is $\geq p^n$ where n is the p-nilpotence degree of X.*

Proof. Put

$$\mathfrak{w} = \{Y \in \mathfrak{v} \mid \mathrm{Ad}(u)Y = Y \text{ for all } u \in R(X)\},$$

and

$$W = \{y \in \mathrm{V} \mid u^{-1}yu = y \text{ for all } u \in R(X)\}.$$

Then $\mathfrak{w}$ is a linear subspace of $\mathfrak{v}$, and $\varepsilon(\mathfrak{w}) = W$. This shows that W is a connected subgroup of V.

Denoting by $\mathfrak{z}$ the Lie algebra of Z, we have $\mathfrak{z} \subset \mathfrak{w}$ since any u in $R(X)$ centralizes X by definition. Similarly, we have $Z \subset W$. On the other hand, if $w \in W$, then $w^{-1}\varepsilon(X)w = \varepsilon(X)$ since $\varepsilon(X) \in R(X)$; this shows that $\mathrm{Ad}(w)X = X$ hence $w \in R(X)$. Since w commutes with each element of $R(X)$, we deduce that $w \in Z$ hence $Z = W$. This shows that Z is connected, and that $\dim \mathfrak{z} = \dim Z = \dim W = \dim \mathfrak{w}$ so that $\mathfrak{z} = \mathfrak{w}$. Since $X \in \mathfrak{w}$, we get $X \in \mathfrak{z}$ and (1) follows.

To see the second assertion of the corollary, one applies Proposition 3.6. □

6.2. We can now prove the *Order Formula* for unipotent elements originally obtained by D. Testerman in [Tes95].

Theorem. (Order Formula) *Let $m \geq 1$ be the minimal integer with $p^m \geq n(P)$, as in Theorem 5.4. Then the exponent of the group* V *is p^m, and the order of a Richardson element of* V *is p^m.*

Proof. In view of Lemma 4.3, we may suppose that G satisfies the hypothesis of Proposition 5.2 and of Proposition 6.1.

Let $Z \leq \mathrm{V}$ be as in Corollary 6.1. Then that corollary together with Theorem 5.4 imply that

$$p^m \leq \text{exponent of } Z \leq \text{exponent of } \mathrm{V} \leq p^m$$

whence equality holds. □

Example. Let G be a group of type G_2, and let $p \geq 5$, so that p is good for G. There are two distinguished orbits of nilpotent (and unipotent) elements; these are usually labelled G_2 (for the regular class) and $G_2(a_1)$ (for the subregular class). We choose a fixed Borel subgroup B; a Richardson element for B represents the regular class. If P is a minimal parabolic subgroup containing B, a Richardson element for P represents the subregular class. Moreover, P is distinguished only if $P = P_\alpha$ where α is the short simple root. We have $n(B) = h = 6$ and $n(P_\alpha) = 3$. A subregular unipotent element always has order p and a subregular nilpotent element is p-nilpotent. A regular unipotent element has order p unless $p = 5$ in which case it has order 25; likewise, a regular nilpotent element is p-nilpotent unless $p = 5$ in which case it has 5-nilpotence degree 2.

Remark. One can compute the order of an arbitrary unipotent u by finding a pair L, Q where $\mathsf{L} \leq G$ is a Levi subgroup containing u and Q is a distinguished parabolic subgroup of L for which u is a Richardson element. Similar remarks hold for an arbitrary nilpotent X.

7. Exponentials in Linear Algebraic Groups

7.1. Exponentials in characteristic 0. Let F be a field of characteristic 0, and let G be a linear algebraic group defined over F. For any nilpotent element $X \in \mathfrak{g}_{\mathsf{F}}$ (the F-form of $\mathfrak{g} = \mathrm{Lie}(G)$) and any rational representation (ρ, V) of G, $d\rho(X)$ is nilpotent so one may define a homomorphism of algebraic groups

$$\varepsilon_{X,V} : \mathbb{G}_a \to \mathrm{GL}(V) \quad \text{via } t \mapsto \exp(d\rho(tX))$$

by the usual formula. If (ρ, V) is defined over F, then so is $\varepsilon_{X,V}$.

Proposition. *There is a unique homomorphism of algebraic groups $\varepsilon_X : \mathbb{G}_a \to G$ such that $\varepsilon_{X,V} = \rho \circ \varepsilon_X$ for all rational representations (ρ, V) of G. The homomorphism ε_X is defined over F.*

Proof. Let (ρ, V) be a faithful F-representation of G. Since the image of $d\varepsilon_{X,V}$ is a subalgebra of $d\rho(\mathfrak{g}_{\mathsf{F}}) \subset \mathfrak{gl}(V)$, one gets $\varepsilon_{X,V}(\mathbb{G}_a) \leq \rho(G) \leq \mathrm{GL}(V)$ by [Bor91, Cor. 6.12]; thus we get a morphism $\varepsilon_X : \mathbb{G}_a \to G$ defined over F and satisfying $\rho \circ \varepsilon_X = \varepsilon_{X,V}$. A second application of the result of *loc. cit.* shows that $\rho' \circ \varepsilon_X = \varepsilon_{X,V'}$ for any rational representation (ρ', V'). Unicity of ε_X is clear. □

7.2. Exponentials over integers. Let A be a Dedekind domain, with field of fractions F. We suppose that F has characteristic 0. [Important examples of A for us are: the rational integers $\mathbb{Z}$, the ring of integers in a number field F, a localization of a Dedekind domain at a prime ideal].

Let G_{F} denote a linear algebraic group over F, with a faithful F-representation (ρ, V). Fix an A-lattice $\mathcal{L} \subset V$; thus $\mathcal{L}$ is a finitely generated A-module containing an F-basis of V. If we localize at a maximal ideal $\mathfrak{m}$, then $\mathcal{L}_{\mathfrak{m}}$ is a free $A_{\mathfrak{m}}$ module; thus $\mathcal{L}$ is A-projective.

Let $J \lhd \mathsf{F}[\mathrm{GL}(V)]$ denote the ideal defining G_{F} (more precisely: defining $\rho(G_{\mathsf{F}})$). The choice of A-lattice $\mathcal{L}$ determines the integral form $A[\mathrm{GL}(\mathcal{L})] \subset \mathsf{F}[\mathrm{GL}(V)]$; let $J_A = J \cap A[\mathrm{GL}(\mathcal{L})]$.

We make the following assumption:

(1) The A-algebra $B = A[\mathrm{GL}(\mathcal{L})]/J_A$ represents a group scheme G_A.

Proposition. *Let H_A be an affine group scheme over A such that $A[H_A]$ is free as an A-module. Let $\phi : H_A \to \mathrm{GL}(\mathcal{L})$ be a homomorphism of group schemes. If the base-changed map ϕ_{F} determines a morphism $H_{\mathsf{F}} \to G_{\mathsf{F}}$, then ϕ determines a morphism $H_A \to G_A$.*

Proof. ϕ is determined by its comorphism $\phi^* : A[\mathrm{GL}(\mathcal{L})] \to A[H_A]$; the proposition will follow if we show that $\phi^*(J_A) = 0$. Note that $\mathsf{F}[\mathrm{GL}(V_{\mathsf{F}})] \simeq A[\mathrm{GL}(\mathcal{L})] \otimes_A \mathsf{F}$ and $\mathsf{F}[H_{\mathsf{F}}] = A[H_A] \otimes_A \mathsf{F}$ (the latter by definition). The comorphism ϕ^*_{F} is then $\phi^* \otimes 1$. The hypothesis implies that $\phi^*_{\mathsf{F}}(J) = 0$; since $A[H_A]$ is free as an A-module, the natural map $A[H_A] \to \mathsf{F}[H_{\mathsf{F}}]$ is injective, and it then follows that $\phi^*(J_A) = 0$ as desired. □

Corollary. *Let $X \in \mathfrak{g}_{\mathsf{F}}$ be nilpotent, and suppose that $d\rho(X) \in \mathrm{End}_A(\mathcal{L})$.*

(a) *Suppose that* $\exp(d\rho(X))\mathcal{L} \subset \mathcal{L}$. *Then the exponential homomorphism*

$$t \mapsto \exp(d\rho(tX)) : \mathbb{G}_{a,A} \to \mathrm{GL}(\mathcal{L})$$

determines a homomorphism of group schemes $\mathbb{G}_{a,A} \to G_A$ *over* A.

(b) *Let* p *be a rational prime, and let* $\mathfrak{m} \lhd A$ *be a maximal ideal for which* $A/\mathfrak{m}$ *has characteristic* p. *Suppose that* $d\rho(X)^{p^i} \in d\rho(\mathfrak{g}_\mathrm{F})$ *for* $0 \leq i < n$, *and that* $d\rho(X)^{p^n} = 0$. *Then the Artin-Hasse exponential map (see 3.2)*

$$\vec{t} \mapsto E_{d\rho(X)}(\vec{t}) : \mathsf{W}_{n,A_\mathfrak{m}} \to \mathrm{GL}(\mathcal{L}_\mathfrak{m})$$

determines a homomorphism of group schemes $\mathsf{W}_{n,A_\mathfrak{m}} \to G_{A_\mathfrak{m}}$ *over* $A_\mathfrak{m}$.

Proof. Note first that the coordinate algebras $A[\mathbb{G}_a]$ and $A[\mathsf{W}_n]$ are free as A modules. (a) follows immediately from the proposition combined with Proposition 7.1. For (b), Lemma 3.3(1) combined with Proposition 7.1 shows that $E_{d\rho(X)}$ determines on base change a morphism $\mathsf{W}_{n,\mathrm{F}} \to G_\mathrm{F}$; the result then follows from the proposition. □

7.3. Nilpotent orbits and fields of definition. If $k \subset k'$ are two algebraically closed fields, then an algebraic group G_k over k determines by extension of scalars an algebraic group $G_{k'}$ over k'. Suppose that G_k acts on an affine variety V_k; $G_{k'}$ also acts on $V_{k'}$.

The following result is attributed to P. Deligne in the introduction to G. Lusztig's paper "On the finiteness of the number of unipotent classes," [Invent. Math. 34 (1976)]. A proof due to R. Guralnick can be found in [GLMS97, Prop 1.1].

Proposition. *Suppose that* G_k *has finitely many orbits on* V_k. *Then* $G_{k'}$ *has finitely many orbits on* $V_{k'}$, *and each* $G_{k'}$ *orbit has a* k*-rational point. In particular, the number of* G_k *orbits on* V_k *is the same as the number of* $G_{k'}$ *orbits on* $V_{k'}$.

Richardson's theorem [Hum95, Theorem 3.10] (together with case-by-case analysis for bad primes – see the discussion in *loc. cit.* Theorem 6.19) shows that a reductive group has finitely many orbits on its nilpotent variety, so we obtain:

Corollary. *If* G *is a reductive group over an algebraically closed field* k, *then each nilpotent orbit of* G *in* $\mathfrak{g}$ *contains a point which is rational over the algebraic closure of the prime field in* k.

Remark. When $p = 0$ or is sufficiently large for the reductive group G, it follows from [SS70, Theorem III.4.29] that each nilpotent orbit has a point rational over the prime field. We don't need this fact.

7.4. Exponentials and Chevalley groups. We have already mentioned in 5.2 the existence of a split reductive group scheme $G_\mathbb{Z}$ over $\mathbb{Z}$ from which G arises by base change; we now need more precise information about $G_\mathbb{Z}$.

We suppose G to be a semisimple group over k. Then G is (isomorphic with) a Chevalley group; we recall some of the ideas behind this construction (for which the reader may find full details in [Ste68]).

Let $\mathfrak{g}_\mathbb{Q}$ denote a split simple Lie algebra over $\mathbb{Q}$ with the same root system as G. For a suitable finite dimensional $\mathbb{Q}$-representation $(d\rho, V)$ of $\mathfrak{g}_\mathbb{Q}$, and a $\mathbb{Z}$-lattice $\mathcal{L} \subset V$ invariant by Kostant's $\mathbb{Z}$-form of the enveloping algebra of $\mathfrak{g}_\mathbb{Q}$, one "exponentiates" the action of Chevalley basis elements on $\mathcal{L}$ to obtain Chevalley groups with the following properties:

- Over $\mathbb{Q}$, one gets a closed subgroup $G_{\mathbb{Q}} \leq \mathrm{GL}(V)$ defined and split semisimple over $\mathbb{Q}$. The root datum of $G_{\mathbb{Q}}$ is the same as that of G. Moreover, the $\mathbb{Q}$-Lie algebra of $G_{\mathbb{Q}}$ is $\mathfrak{g}_{\mathbb{Q}}$.
- In characteristic $p > 0$, one gets a closed subgroup $G_{\mathbb{F}_p} \leq \mathrm{GL}(\mathcal{L}/p\mathcal{L})$, defined and split semisimple over $\mathbb{F}_p$, which is isomorphic over k with the original group G.

Since there should be no danger of confusion, we will write (ρ, V) for the representation of $G_{\mathbb{Q}}$ on V, and $(\rho, \mathcal{L}/p\mathcal{L})$ for the representation of $G_{\mathbb{F}_p}$ on $\mathcal{L}/p\mathcal{L}$.

As in 7.2, let $J \lhd \mathbb{Q}[\mathrm{GL}(V)]$ be the ideal defining the $\mathbb{Q}$-variety G, and put $J_{\mathbb{Z}} = J \cap \mathbb{Z}[\mathrm{GL}(\mathcal{L})]$ (where $\mathbb{Z}[\mathrm{GL}(\mathcal{L})]$ is regarded as a subring of $\mathbb{Q}[\mathrm{GL}(V)]$ in the obvious way). Let B be the $\mathbb{Z}$-algebra $\mathbb{Z}[\mathrm{GL}(\mathcal{L})]/J_{\mathbb{Z}}$.

Lemma. *The $\mathbb{Z}$-algebra B represents a split semisimple group scheme $G_{\mathbb{Z}}$ over $\mathbb{Z}$. One has $B \otimes_{\mathbb{Z}} \mathbb{F}_p = \mathbb{F}_p[G_{\mathbb{F}_p}]$ and $B \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}[G_{\mathbb{Q}}]$, or equivalently, $G_{\mathbb{Q}}$ and $G_{\mathbb{F}_p}$ are obtained by base change from $G_{\mathbb{Z}}$.*

Proof. This is proved in [Bor70, §3.4 and §4]. □

Let now A be a Dedekind domain with field of fractions F as in 7.2. We suppose that F is a finite extension of $\mathbb{Q}$ (so F is a number field). We regard F as a subfield of a fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. Let G_A be the group scheme obtained from $G_{\mathbb{Z}}$ by base change; thus G_A is represented by

$$B \otimes_{\mathbb{Z}} A = A[\mathrm{GL}(\mathcal{L} \otimes_{\mathbb{Z}} A)]/J_A \tag{1}$$

[where J_A is the ideal $\mathsf{F}J \cap A[\mathrm{GL}(\mathcal{L}_A)]$ with the intersection occurring in $\mathsf{F}[\mathrm{GL}(V_{\mathsf{F}})]$.]

The choice of a Chevalley basis of $\mathfrak{g}_{\mathbb{Q}}$ entails the choice of a triangular decomposition $\mathfrak{g}_{\mathbb{Q}} = \mathfrak{u}_{\mathbb{Q}}^- \oplus \mathfrak{h}_{\mathbb{Q}} \oplus \mathfrak{u}_{\mathbb{Q}}$ where $\mathfrak{h}_{\mathbb{Q}}$ is a maximal toral subalgebra; the construction of $G_{\mathbb{Q}}$ yields also a maximal torus $T_{\mathbb{Q}} \leq G_{\mathbb{Q}}$ with $\mathrm{Lie}(T_{\mathbb{Q}}) = \mathfrak{h}_{\mathbb{Q}}$. Moreover, we have the decomposition $\mathfrak{g}_{\mathbb{Z}} = \mathfrak{u}_{\mathbb{Z}}^- \oplus \mathfrak{h}_{\mathbb{Z}} \oplus \mathfrak{u}_{\mathbb{Z}}$, where e.g. $\mathfrak{u}_{\mathbb{Z}}$ is the $\mathbb{Z}$-span of the Chevalley basis elements which correspond to the positive roots.

Let $\phi = \sum_{\alpha > 0} \alpha^\vee$ regarded as a cocharacter for the torus $T_{\mathbb{Q}}$. To the $\mathfrak{g}_{\mathbb{Q}}$ module V, we associate the integer

$$n(V) = \max\{\langle \lambda, \phi \rangle \mid \lambda \in X^*(T_{\mathbb{Q}}),\ V_\lambda \neq 0\}.$$

Proposition. (1) *If $X \in \mathfrak{g}_{\overline{\mathbb{Q}}}$ is nilpotent, then $d\rho(X)^{n(V)+1} = 0$.*

(2) *Suppose $X \in \mathfrak{g}_{\mathsf{F}}$ is nilpotent and satisfies $d\rho(X)\mathcal{L}_A \subset \mathcal{L}_A$. If $n(V)!$ is invertible in A (e.g. if A is local with residue field of characteristic $p > n(P)$), then $\exp(d\rho(X))$ leaves $\mathcal{L}_A$ invariant and $t \mapsto \exp(d\rho(tX))$ defines a morphism of group schemes $\mathbb{G}_{a,A} \to G_A$.*

Proof. (1). We may suppose that $X \in \mathfrak{u}_{\overline{\mathbb{Q}}}$. The co-character ϕ induces a grading on $V_{\overline{\mathbb{Q}}}$ by $V_i = \{v \in V_{\overline{\mathbb{Q}}} \mid \rho(\phi(t))v = t^i v\ \forall t \in \overline{\mathbb{Q}}\}$; evidently $d\rho(X)$ acts as a sum of homogeneous terms of positive and even degree. Since the Weyl group of $\mathfrak{g}_{\mathbb{Q}}$ permutes the weights of V, it follows that $V_{\overline{\mathbb{Q}}} = \bigoplus_{-n(V) \leq i \leq n(V)} V_i$, and (1) is then immediate. [One can alternately argue that the graded components of $V_{\overline{\mathbb{Q}}}$ are the weight spaces for the action of an $\mathfrak{sl}_2$-subalgebra containing a regular nilpotent element, so that $n(V)$ is the highest weight. Since the regular nilpotent elements are dense in the nilpotent variety, (1) follows; moreover, this argument shows that $d\rho(X)^{n(V)} \neq 0$ when X is regular.]

(2) Since $i!$ is invertible in A for each $0 \le i \le n(V)$ and since $d\rho(X)^{n(V)+1} = 0$ by (1), it follows that $\exp(d\rho(X))$ leaves $\mathcal{L}_A$ invariant. The result now holds by Corollary 7.2(a). □

Corollary. *Suppose that $n(V) < p$ and that $X \in \mathfrak{g}_k$ is nilpotent. Then $X^{[p]} = 0$, and the (truncated) exponential $t \mapsto \exp(d\rho(tX))$ defines a morphism of algebraic groups $\mathbb{G}_{a,k} \to G = G_k$.*

Proof. In view of the results of 7.3, we may suppose that k is an algebraic closure of the finite field $\mathbb{F}_p$.

The image of $\mathfrak{u}_{\mathbb{Z}}$ in $\mathfrak{g}_{\mathbb{F}_p}$ is the $\mathbb{F}_p$-Lie algebra of the unipotent radical of a Borel subgroup. Since k is an algebraic closure of $\mathbb{F}_p$, there is a finite extension F of $\mathbb{Q}$ and a valuation ring A in F whose residue field $A/\mathfrak{m} = l \subset k$ has the property that $\mathrm{Ad}(g)X \in \mathfrak{u}_l$ for a suitable $g \in G(l)$. Thus, we may suppose $X \in \mathfrak{u}_l$. Since $\mathfrak{u}_l = \mathfrak{u}_A/\mathfrak{m} \cdot \mathfrak{u}_A$, we may choose a lift $\tilde{X} \in \mathfrak{u}_A$ of X. Since each element of $\mathfrak{u}_{\mathsf{F}}$ is nilpotent, part (1) of the previous proposition now shows that $d\rho(\tilde{X})^p = 0$, hence also $d\rho(X)^p = 0$ which implies $X^{[p]} = 0$.

Since $n(V)$ is invertible in A, part (2) of the previous proposition shows that the exponential map determines a morphism of group schemes $\varepsilon : \mathbb{G}_{a,A} \to G_A$ over A. The condition $d\rho(\tilde{X})^p = 0$ implies that $\rho \circ \varepsilon$ has degree $< p$ when regarded as a morphism of F-varieties $\mathbb{G}_{a,\mathsf{F}} = \mathbb{A}^1 \to \mathrm{GL}(V)$. Denoting by $\overline{\varepsilon} : \mathbb{G}_{a,k} \to G_k$ the morphism obtained by base change, it follows that also $\rho \circ \overline{\varepsilon}$ has degree $< p$.

The differential $d\varepsilon : \mathsf{F} = \mathrm{Lie}(\mathbb{G}_{a,\mathsf{F}}) \to \mathfrak{g}_{\mathsf{F}}$ satisfies $d\varepsilon(1) = \tilde{X}$. It follows that $d(\rho \circ \overline{\varepsilon})(1) = d\rho(X)$.

Now, the exponential through $d\rho(X)$ is the unique homomorphism $\mathbb{G}_{a,k} \to \mathrm{GL}(\mathcal{L}_A \otimes_A k)$ with degree $< p$ and whose differential at 1 is $d\rho(X)$. Thus, $\overline{\varepsilon}$ coincides with the truncated exponential, and the corollary is proved. □

Remarks. (1) Suppose that G is of adjoint type (i.e. that the character group of a maximal torus is spanned over $\mathbb{Z}$ by the roots). Then G arises as a Chevalley group where we may take the adjoint module $(\mathrm{ad}, \mathfrak{g}_{\mathbb{Q}})$ for the $\mathfrak{g}_{\mathbb{Q}}$ module $(d\rho, V)$. In this case, one has $n(\mathfrak{g}_{\mathbb{Q}}) = 2h - 2$ where h is the Coxeter number of the root system of G (see [Car93, Prop. 5.5.2]).

The reader should compare the result of the Corollary in this case with [Car93, Prop. 5.5.5(iv)], where a similar conclusion is asserted, but with the weaker bound $p > 3h-3$. We emphasize that the argument doesn't depend on the Bala-Carter theorem. We have used the finiteness of nilpotent orbits in order to know that every nilpotent orbit has a rational point over the algebraic closure of a finite field; as noted before, in good characteristic that finiteness is a result of Richardson and is independent of the classification of nilpotent orbits.

(2) We will be most interested in applying the corollary in case G is quasisimple with exceptional root system. We list here some data for these root systems, including the minimal dimensional non-trivial $\mathfrak{g}_{\mathbb{Q}}$ module V_{min}. The module V_{min} is a simple module $L_{\mathbb{Q}}(\lambda)$ with highest λ; we describe λ in terms of the fundamental dominant weights with the labelling as in the tables in [Bou72, Planche V-IX]. Those tables may be used to compute the

indicated values of $n(V_{\text{min}}) = \langle \lambda, \varphi \rangle$.

R	$2h-2$	V_{min}	$n(V_{\text{min}})$
G_2	10	$L_{\mathbb{Q}}(\varpi_1)$	6
F_4	22	$L_{\mathbb{Q}}(\varpi_4)$	16
E_6	22	$L_{\mathbb{Q}}(\varpi_1)$	16
E_7	34	$L_{\mathbb{Q}}(\varpi_7)$	27
E_8	58	$L_{\mathbb{Q}}(\varpi_8)$	58

(3) The technique used in proof of the Theorem is similar to that used in [Tes95]. Let $Y \in \mathfrak{g}_{\mathbb{Q}}$ with $d\rho(Y) \in \mathrm{End}_{\mathbb{Z}_{(p)}}(\mathcal{L})$. We remark that [Tes95, Lemma 1.4] gives moreover a condition under which $\exp(d\rho(Y))$ leaves invariant the lattice $\mathcal{L}$ even when $d\rho(Y)^p \neq 0$. We mention also a different condition: namely, $(*)$ if $d\rho(Y)^p\mathcal{L} \subset p\mathcal{L}$ and $d\rho(Y)^{p^2} = 0$ then $\exp(d\rho(Y))$ leaves $\mathcal{L}_{\mathbb{Z}_{(p)}}$ invariant. This follows from the formula for $\nu_p(i!)$ which may be found in [Kob77, Ch. I, Exerc. 13c].

The condition $d\rho(Y)^p\mathcal{L} \subset p\mathcal{L}$ means that the image $\overline{Y}$ of Y in $\mathfrak{g}_k$ is p-nilpotent; one may argue, as in the corollary, that under the condition $(*)$ there is a homomorphism $\mathbb{G}_a \to G$ over k obtained by base change from the exponential over $\mathbb{Z}_{(p)}$. However, the homomorphism over $\mathbb{Z}_{(p)}$ need not have degree $< p$; thus the map obtained by reduction modulo p need not coincide with the truncated exponential of $\overline{Y}$ in $\mathrm{GL}(\mathcal{L}/p\mathcal{L})$.

7.5. Classical groups and the Artin-Hasse exponential. Let V be a $\mathbb{Q}$-vector space with a bilinear form φ. Let $G_{\mathbb{Q}}$ be the stabilizer in $\mathrm{SL}(V)$ of φ. We assume that one of the following three statements holds:

CG1. $\varphi = 0$, so that $G_{\mathbb{Q}} = \mathrm{SL}(V)$

CG2. φ is non-degenerate and alternating, so that $G_{\mathbb{Q}} = \mathrm{Sp}(V, \varphi)$,

CG3. φ is non-degenerate and symmetric, so that $G_{\mathbb{Q}} = \mathrm{SO}(V, \varphi)$. Moreover, if $\dim_{\mathbb{Q}} V$ is written as $2r+\epsilon$ with $\epsilon \in \{0, 1\}$, then V contains a totally singular $\mathbb{Q}$-subspace of dimension r (so φ has maximal Witt index, or is a *split form*).

In each case, $G_{\mathbb{Q}}$ is a connected, quasisimple $\mathbb{Q}$-split group.

The Lie algebra $\mathfrak{g}_{\mathbb{Q}}$ of $G_{\mathbb{Q}}$ is split simple, and we may carry out the "Chevalley group" constructions of 7.4 for $\mathfrak{g}_{\mathbb{Q}}$ with respect to its natural representation (ν, V). Fix a lattice $\mathcal{L} \subset V$ invariant by $\mathcal{U}_{\mathbb{Z}}$. Over $\mathbb{Q}$, the group constructed in this way identifies with the original group $G_{\mathbb{Q}}$; this follows from [Ree57]. For each prime p, we get also a quasisimple $\mathbb{F}_p$-split algebraic group $G_{\mathbb{F}_p}$ with the same root datum as $G_{\mathbb{Q}}$.

The formal character of the $G_{\mathbb{F}_p}$-representation $(\nu, \mathcal{L}/p\mathcal{L})$ coincides with the formal character of the $G_{\mathbb{Q}}$-representation (ν, V); moreover, it is well known that $G_{\mathbb{F}_p}$ has an irreducible representation with that formal character (provided $p \neq 2$ in case CG3 with $\epsilon = 1$). Thus $\mathcal{L}/p\mathcal{L}$ is irreducible for $G_{\mathbb{F}_p}$ (with this restriction on p).

Replacing φ by a suitable integral multiple, we may suppose in case CG2 or CG3 that $\varphi(\mathcal{L}, \mathcal{L}) = \mathbb{Z}$; note that the group $G_{\mathbb{Q}}$ and Lie algebra $\mathfrak{g}_{\mathbb{Q}}$ are unchanged by this replacement. For each prime p (with the restriction on p of the previous paragraph), φ induces a non-0 bilinear form $\overline{\varphi}$ on $\mathcal{L}/p\mathcal{L}$; since that module is irreducible, $\overline{\varphi}$ must be non-degenerate. It then follows from [Ree57] that $G_{\mathbb{F}_p}$ coincides with the stabilizer in $\mathrm{SL}(\mathcal{L}/p\mathcal{L})$ of $\overline{\varphi}$ so long as $p \neq 2$ in case CG3 (for either value of ϵ).

Let $B = \mathbb{Z}[\mathrm{GL}(\mathcal{L})]/J_{\mathbb{Z}}$ as in 7.4. Then B represents a group scheme over $\mathbb{Z}$, and for each prime integer p, it follows from Lemma 7.4 that $B \otimes_{\mathbb{Z}} \mathbb{F}_p$ is the coordinate ring of $G_{\mathbb{F}_p}$.

Lemma. *Let n be a positive integer, and suppose that n is odd in case (ii) or (iii). Let F be an extension field of $\mathbb{Q}$. If $X \in \mathfrak{g}_{\mathsf{F}}$, then $d\nu(X)^n \in d\nu(\mathfrak{g}_{\mathsf{F}})$.*

Proof. We have for each $v, w \in V_{\mathsf{F}}$:

$$\varphi(d\nu(X)^n v, w) = (-1)^n \varphi(v, d\nu(X)^n w),$$

whence the result. □

We now deduce in this case a recent result of R. Proud:

Proposition. *Suppose that p is good for G_k (i.e. that $p \neq 2$ in case CG2 or CG3). For each nilpotent $X \in \mathfrak{g}$ with p-nilpotence degree n, the Artin-Hasse exponential defines an injective morphism of algebraic groups $E_X : W_n \to G_k$. Thus each unipotent element of G lies in a closed subgroup isomorphic with some W_n. If l is a subfield of k and $X \in \mathfrak{g}_l$ then E_X is defined over l.*

Proof. Using the results of 7.3, we may suppose that k is an algebraic closure of the finite field $\mathbb{F}_p$. As in the proof of Corollary 7.4, we may find a number field F with valuation ring A and residue field $l = A/\mathfrak{m}$ for which X lies in $\mathfrak{u}_l$ (where $\mathfrak{u}_{\mathbb{Z}}$ is the $\mathbb{Z}$-span of suitable Chevalley basis elements, as before). Thus we may choose a lift $\tilde{X} \in \mathfrak{u}_A$ of $X \in \mathfrak{u}_l = \mathfrak{u}_A/\mathfrak{m}\mathfrak{u}_A$.

Corollary 7.2(b) now yields a homomorphism of group schemes $E_{\tilde{X}} : W_{m,A} \to G_A$ given by the Artin-Hasse exponential, where $m \geq n$ is the nilpotence degree of $d\nu(\tilde{X})$.

We get then by base change a homomorphism $W_{m,k} \to G_k$ over k; note that by the formula defining $E_{\tilde{X}}$ in 3.3, this base-changed homomorphism vanishes on the subgroup $K = \{(0, \dots, 0, t_n, \dots, t_{m-1})\} \leq W_{m,k}$, and coincides with the homomorphism $E_{d\nu(X)} : W_{m,k}/K = W_{n,k} \to \mathrm{GL}(V)$. It follows that $E_{d\nu(X)}$ takes values in G_k (hence has rights to be called E_X), and is injective, as claimed.

It is clear that the partition of $\dim V$ determined by the Jordan block sizes of the unipotent element $\nu(E_X(1))$ on the natural module V is the same as the partition of $d\nu(X)$. In the cases CG1, CG2 and CG3 with $\epsilon = 1$, the unipotent classes of G and nilpotent classes of $\mathfrak{g}$ are classified by these partitions (see [Hum95, 7.11]), so we get the claim on unipotent elements in these cases. In case CG3 with $\dim V$ even, let $G' = O(\mathcal{L} \otimes_A k)$ denote the full orthogonal group; thus G is the identity component of G', and has index 2. The unipotent elements of G' all lie in G, and $\mathrm{Lie}(G) = \mathrm{Lie}(G')$. Again by [Hum95, 7.11], the unipotent and nilpotent classes of G' are classified by partition, so it is clear that each unipotent element of G' lies in a suitable Witt-vector subgroup. But any such subgroup, being connected, must lie in G.

The rationality assertion is clear. □

R. Proud has proved the proposition for *all* quasisimple groups G, not only classical groups; see [Pro]. His techniques for classical G are different from those used here.

8. THE EXPONENTIAL ISOMORPHISM FOR $p \geq n(P)$

We describe in this section an argument due to Serre [Ser96, §2.2] that will be used below. This argument is also used in some recent work of Gary Seitz [Sei00, §5].

Suppose $B_{\mathbb{Z}}$ is a Borel subgroup of the split reductive group $G_{\mathbb{Z}}$ over $\mathbb{Z}$, and let $B \leq G$ be the corresponding groups over k. For $\alpha \in R$, let ϕ_α be an isomorphism over $\mathbb{Z}$ between $\mathbb{G}_a$ and the root subgroup $U_\alpha \leq B$.

Any standard parabolic subgroup $B \leq P \leq G$ is defined over $\mathbb{Z}$. If V denotes the unipotent radical of P, then the ϕ_α define an isomorphism $\prod_{\alpha \in R \setminus R_I} U_{\alpha,\mathbb{Z}} \to$ $\mathrm{V}_{\mathbb{Z}}$ of schemes over $\mathbb{Z}$ (where $I \subset S$ defines the parabolic subgroup P as in 4.3). For any $\mathbb{Z}$-algebra Λ, a point u of V over $\mathbb{Z}$ may thus be written uniquely as $u = \prod_{\alpha \in R \setminus R_I} \phi_\alpha(t_\alpha)$ with $t_\alpha \in \Lambda$; thus the t_α form a system of coordinates for V over $\mathbb{Z}$.

The Lie algebra $\mathfrak{v}_{\mathbb{Z}}$ is the $\mathbb{Z}$-span of the $e_\alpha = d\phi_\alpha(1)$ for $\alpha \in R^+ \setminus R_I^+$. The nilpotence degree $n = n(P)$ of $\mathrm{V}_{\mathbb{Q}}$ (and of $\mathfrak{v}_{\mathbb{Q}}$) is given by the formula in 4.4; we will work with the ring $A = \mathbb{Z}[1/(n-1)!]$.

Proposition 7.1 implies that the exponential map defines a morphism of varieties $\varepsilon : \mathfrak{v}_{\mathbb{Q}} \to \mathrm{V}_{\mathbb{Q}}$ over $\mathbb{Q}$. Similarly, the logarithm yields a morphism of varieties $\mathrm{V}_{\mathbb{Q}} \to \mathfrak{v}_{\mathbb{Q}}$, so that ε is an isomorphism. For each $\mathbb{Q}$-algebra Λ, each Λ-point u of V may be written uniquely as $u = \varepsilon(\sum_{\alpha \in R \setminus R_I} u_\alpha e_\alpha)$ for $u_\alpha \in \Lambda$. Thus the u_α form a system of coordinates for V over $\mathbb{Q}$.

Since $\mathfrak{v}_{\mathbb{Q}}$ is a nilpotent Lie algebra, it may be regarded as an algebraic group over $\mathbb{Q}$ via the Hausdorff series (compare [Ser96, 2.2] for the case $P = B$, and see [Bou89, Ch. 2, §6]). Moreover, it follows from [Bou89, ch. 2 §6.4 Theorem 2] that the operation in $\mathfrak{v}_{\mathbb{Q}}$ is defined over A, so that $\mathfrak{v}_A$ is an affine group scheme over A.

Theorem. *The exponential map ε defines a P_A-equivariant isomorphism of group schemes $\mathfrak{v}_A \to \mathrm{V}_A$.*

Proof. The essential point is proved in [Ser96, §2.2, Prop. 1] for $P = B$; the generalization to P is immediate. One observes as in *loc. cit.* that

$$u_\alpha = t_\alpha + P_\alpha((t_\beta)_{\beta < \alpha})$$

where P_α is a polynomial with coefficients in $A = \mathbb{Z}[1/(n-1)!]$ in the t_β with $\beta < \alpha$. It follows that ε is an isomorphism over A (see [Ser96, §2.2, Rem. 2]). The equivariance assertion is clear. □

Example. Let $G = \mathrm{Sp}_4(\mathbb{Q})$, so that R is of type C_2, and let $P = B$. Recall that $R^+ = \{\alpha, \beta, \alpha+\beta, 2\alpha+\beta\}$. It is straightforward to check that

$$\varepsilon(X) = \phi_\alpha(a)\phi_\beta(b)\phi_{\alpha+\beta}\left(c + \frac{ab}{2}\right)\phi_{2\alpha+\beta}\left(d - bc - \frac{2ab^2}{3}\right)$$

for $X = ae_\alpha + be_\beta + ce_{\alpha+\beta} + de_{2\alpha+\beta}$. It is then clear that exp is an isomorphism over $A = \mathbb{Z}[1/6]$ (note that $h - 1 = n(B) - 1 = 3$).

If $p \geq n(P)$, then the field k is an A algebra (in a unique way), and the above result yields the following:

Corollary. *Suppose that $p \geq n(P)$.*

1. *ε is a P-equivariant isomorphism of k-varieties $\mathfrak{v} \to \mathrm{V}$.*
2. *If $X, Y \in \mathfrak{v}$ satisfy $[X, Y] = 0$, then $\varepsilon(X)$ and $\varepsilon(Y)$ commute.*

Proof. (1) is immediate. For (2), one must note that the condition $[X, Y] = 0$ implies that X and Y commute when $\mathfrak{v}$ is regarded as a group by the Hausdorff series. □

Remark. If $p \geq h$, then ε defines an isomorphism $\mathfrak{u} \to U$. Since $\varepsilon(X)^p = \varepsilon(pX) = 1$ for any $X \in \mathfrak{u}$, this gives yet another proof that every unipotent $u \in G$ satisfies $u^p = 1$ when $p \geq h$.

9. Cohomology of Frobenius kernels

9.1. Let H be a linear algebraic groups over the algebraically closed field k. For $d \geq 1$, denote by H_d the d-th Frobenius kernel; see [Jan87, I.9] for the a full discussion. We recall some of the details: Let $\mathfrak{m} \lhd k[H]$ be the ideal defining 1 in the group H, and put $\mathfrak{m}_d = \sum_{f \in \mathfrak{m}} k[H] f^{p^d}$. Then H_d is the group scheme represented by the finite dimensional k-algebra $k[H_d] = k[H]/\mathfrak{m}_d$; see [Jan87, I.9.6]. In particular, H_d is an infinitesimal group scheme [Jan87, I.9.6(1)].

(1). *There is are natural bijections*

$$\begin{aligned}\mathrm{Hom}_{\mathrm{gs}}(H_d, H') \simeq \mathrm{Hom}_{\mathrm{gs}}(H_d, {H'}_d) &\simeq \mathrm{Hom}_{\mathrm{Hopf}}(k[{H'}_d], k[H_d]) \\ &\simeq \mathrm{Hom}_{\mathrm{Hopf}}(\mathrm{Dist}(H_d), \mathrm{Dist}({H_d}')),\end{aligned}$$

where $\mathrm{Hom}_{\mathrm{gs}}$ *refers to homomorphisms of group schemes,* $\mathrm{Hom}_{\mathrm{Hopf}}$ *refers to Hopf algebra homomorphisms, and* $\mathrm{Dist}(H_d)$ *denotes the algebra of distributions of* H_d *as in* [Jan87, I.7].

Proof. Since all our group schemes are affine, the homomorphisms between them may be identified with comorphisms on coordinate algebras. The first two isomorphisms follow from this and the fact that for any homomorphism $\phi : H_d \to H'$, the comorphism $\phi^* : k[H'] \to k[H_d]$ vanishes on $\mathfrak{m}'_d$. Since H_d is infinitesimal, $\mathrm{Dist}(H_d)$ identifies with the dual Hopf algebra of $k[H_d]$ by [Jan87, I.8.4]; the last isomorphism follows at once. □

(2). *If A_1 and A_2 are finite dimensional Hopf algebras over k, then* $\mathrm{Hom}_{\mathrm{Hopf}}(A_1, A_2)$ *has a natural structure of algebraic variety over k.*

Proof. Since the A_i are finite dimensional, we regard $X = \mathrm{Hom}_{\mathrm{Hopf}}(A_1, A_2)$ as a subset of the affine space $\mathbb{A} = \mathrm{Hom}_k(A_1, A_2)$ of all k-linear maps. For each $a, b \in A_1$, the map $\lambda_{a,b} : \mathbb{A} \to A_2$ given by $\phi \mapsto \phi(ab) - \phi(a)\phi(b)$ is clearly a morphism of varieties, and the set $X_a \subset \mathbb{A}$ of all algebra homomorphisms is the intersection of all $\lambda_{a,b}^{-1}(0)$, hence is a closed subvariety. One similarly sees that the subset X_c of all coalgebra homomorphisms is closed, and the subset X_{ant} of all antipode preserving linear maps is closed. Then $X = X_a \cap X_c \cap X_{ant}$ is also closed. □

(3). $\mathrm{Hom}_{\mathrm{gs}}(H_d, H') \simeq \mathrm{Hom}_{\mathrm{gs}}(H_d, {H'}_d)$ *has the structure of an H'-variety.*

Proof. The variety structure is evident from the previous remarks. The above identification is compatible with the action of H' on itself by inner automorphisms, and on ${H'}_d$ by the adjoint representation; this action yields the structure of H'-variety. □

9.2. For any linear algebraic group H over k, consider the H-variety

$$\mathcal{A}(d,H) = \operatorname{Hom}_{\mathrm{gs}}(\mathbb{G}_{a,d}, H)$$

of the previous section, where $\mathbb{G}_{a,d}$ is the d-th Frobenius kernel of the additive group. This is the reduced variety corresponding to a certain (possibly not reduced) affine k-scheme $\underline{\mathcal{A}}(d,H)$ appearing in [SFB97a, Theorem 1.5] (where it is called $V_d(H)$).

9.3. Let T be a k-torus with character group $X = X^*(T)$ and co-character group $Y = X_*(T)$. Then T is obtained by base change from the $\mathbb{Z}$-torus $T_{\mathbb{Z}}$ defined by $\mathbb{Z}[X]$.

We now use the results of [Jan87, I.7.8] to describe the algebra of distributions. The $\mathbb{Z}$-algebra $\operatorname{Dist}(T_{\mathbb{Z}})$ is a free $\mathbb{Z}$-module; any $\mathbb{Z}$-basis $H_1, \dots, H_n$ of Y yields a corresponding $\mathbb{Z}$-basis of $\operatorname{Dist}(T_{\mathbb{Z}})$: namely, all products $\prod_{i=1}^n \binom{H_i}{n_i}$ with $n_i \in \mathbb{N}$. We will say that the degree of such a product is $\sum_i n_i$. The distributions of T arise by base change: $\operatorname{Dist}(T) = \operatorname{Dist}(T_{\mathbb{Z}}) \otimes_{\mathbb{Z}} k$.

Distributions in $\operatorname{Dist}(T_{\mathbb{Z}})$ are certain linear forms in $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}[X], \mathbb{Z})$: for $H \in Y$, $n \in \mathbb{N}$ and $\lambda \in X$, we have by definition $\binom{H}{n}(\lambda) = \binom{\langle \lambda, H\rangle}{n}$.

Let now T' (with groups X', Y', etc) be a second k-torus, and suppose that $\phi : T \to T'$ is a morphism. The morphism ϕ induces maps on the character and co-character groups: $\phi^* : X' \to X$ and $\phi_* : Y \to Y'$. In turn, ϕ^* determines a map $\mathbb{Z}[X'] \to \mathbb{Z}[X]$ and hence a morphism $\phi_{\mathbb{Z}} : T_{\mathbb{Z}} \to T'{}_{\mathbb{Z}}$ from which ϕ arises by base change.

Assume that $(*)$ $\phi^* : X' \to X$ is injective and has cokernel a finite group of order prime to p. This guarantees that $\dim T = \dim T'$, ϕ is separable, and $\ker \phi$ is a reduced group scheme.

The map $\operatorname{Dist}(\phi_{\mathbb{Z}}) : \operatorname{Dist}(T_{\mathbb{Z}}) \to \operatorname{Dist}(T'_{\mathbb{Z}})$ may be understood as follows: for $\lambda' \in X'$ we have by definition $\operatorname{Dist}(\phi_{\mathbb{Z}})\left(\binom{H}{n}\right)(\lambda') = \binom{H}{n}(\phi^*\lambda') = \binom{\langle \phi^*\lambda', H\rangle}{n} = \binom{\langle \lambda', \phi_* H\rangle}{n}$. Thus, $\operatorname{Dist}(\phi_{\mathbb{Z}})\left(\binom{H}{n}\right) = \binom{\phi_* H}{n}$.

Lemma. *Under the assumption* $(*)$, $\operatorname{Dist}(\phi) : \operatorname{Dist}(T) \to \operatorname{Dist}(T')$ *is an isomorphism.*

Proof. Condition $(*)$ yields $\mathbb{Z}$-bases $H_1, \dots, H_n$ of Y and $H'_1, \dots, H'_n$ of Y' and integers $a_1, \dots, a_n$ for which $\phi_*(H_i) = a_i H'_i$ and $\prod_i a_i \not\equiv 0 \pmod{p}$.

These bases of Y and Y' determine bases for the respective distribution algebras, and we have $\operatorname{Dist}(\phi_{\mathbb{Z}})\left(\prod_i \binom{H_i}{m_i}\right) = \prod_i \binom{a_i H'_i}{m_i}$. One may check that

$$\prod_i \binom{a_i H'_i}{m_i} = \prod_i a_i^{m_i} \prod_i \binom{H'_i}{m_i} + \mathcal{E},$$

where $\mathcal{E}$ is a $\mathbb{Z}$-linear combinations of basis elements of lower degree. It follows that $\operatorname{Dist}(\phi) = \operatorname{Dist}(\phi_{\mathbb{Z}}) \otimes 1_k$ is an isomorphism, as claimed. □

Theorem. *Let $\phi : G \to G'$ be a central isogeny of connected, semisimple groups over k, as in* [Jan87, Prop. II.1.14]. *Suppose that* $\ker \phi$ *is reduced. Then ϕ induces an isomorphism* $\operatorname{Dist}(G) \simeq \operatorname{Dist}(G')$.

Proof. According to [Jan87, II.1.12(2)], multiplication is an isomorphism

$$\mathrm{Dist}(U^-) \otimes \mathrm{Dist}(T) \otimes \mathrm{Dist}(U) \simeq \mathrm{Dist}(G),$$

where U and U^- are the unipotent radicals of opposite Borel subgroups and T is a maximal torus. Moreover, (see [Jan87, II.1.14]) ϕ induces maps on these tensor factors; it is clear from the description of ϕ that it induces an isomorphism $\mathrm{Dist}(U) \to \mathrm{Dist}(U')$ (with a similar statement for U^-). Thus, it suffices to show that ϕ induces an isomorphism $\mathrm{Dist}(T) \to \mathrm{Dist}(T')$.

Since G and G' are semisimple, $\dim T = \dim T'$; since $X^*(T)_{\mathbb{Q}}$ and $X^*(T')_{\mathbb{Q}}$ are spanned over $\mathbb{Q}$ by the roots, the map ϕ^* on character groups induced by the homomorphism $\phi_{|T} : T \to T'$ is injective; since $\operatorname{coker} \phi$ is reduced, $\ker \phi^*$ has order prime to p. Thus, the lemma shows that $\mathrm{Dist}(\phi_{|T})$ induces an isomorphism $\mathrm{Dist}(T) \to \mathrm{Dist}(T')$, and the result follows. □

The fundamental group of a root system R is the finite group $X_{\mathrm{sc}}/\mathbb{Z}R$, where X_{sc} is the $\mathbb{Z}$-lattice with basis the fundamental dominant weights. The theorem has the following consequence:

Corollary. *Let G be a connected, semisimple group, with root system R. Denote the simply connected cover by $G_{\mathrm{sc}} \to G$. If p does not divide the order of the fundamental group of R, then $\mathcal{A}(d, G_{\mathrm{sc}}) \simeq \mathcal{A}(d, G)$ as G_{sc}-varieties for each $d \geq 1$.*

9.4. Let H a linear algebraic group over k defined over $\mathbb{F}_p$, with Lie algebra $\mathfrak{h}$. Let $\mathcal{N}_p(\mathfrak{h})$ denote the variety of p-nilpotent elements in $\mathfrak{h}$. For $d \geq 1$, put

$$(1) \quad \mathcal{N}_p(d, \mathfrak{h}) = \{(X_0, \dots, X_{d-1}) \mid X_i \in \mathcal{N}_p(\mathfrak{h}),\ [X_i, X_j] = 0 \text{ for } 0 \leq i, j < d\}.$$

We regard $\mathcal{N}_p(d, \mathfrak{h})$ as an H-variety with the following action:

$$h.(X_0, X_1, \dots, X_{d-1}) = (\mathrm{Ad}(h)X_0, \mathrm{Ad}(Fh)X_1, \dots, \mathrm{Ad}(F^{d-1}h)X_{d-1}),$$

where F denotes the Frobenius morphism on H.

We have the following analogue of Theorem 9.3.

Lemma. *Let G be connected, semisimple with root system R and simply connected cover G_{sc}. If p does not divide the order of the fundamental group of R, there is an isomorphism of G_{sc}-varieties $\mathcal{N}_p(d, \mathrm{Lie}(G)) \simeq \mathcal{N}_p(d, \mathrm{Lie}(G_{\mathrm{sc}})$ for each $d \geq 1$.*

Proof. This follows from the observations made in [Hum95, 0.13]. □

The following result was obtained in [SFB97a, Lemma 1.7].

Proposition. *Suppose that H has a faithful rational representation (ρ, V) with the property that $\exp(d\rho(X)) \in H$ for each $X \in \mathcal{N}_p(\mathfrak{h})$, where $\exp(d\rho(X))$ is the (truncated) exponential in $\mathrm{GL}(V)$. Then there is an isomorphism of H-varieties $\mathcal{N}_p(d, \mathfrak{h}) \simeq \mathcal{A}(d, H)$.*

Actually, in *loc. cit.*, one gets an isomorphism of schemes $\underline{\mathcal{N}}_p(d, \mathfrak{h}) \simeq \underline{\mathcal{A}}(d, H)$; for each commutative k-algebra Λ, $\underline{\mathcal{N}}_p(d, \mathfrak{h})(\Lambda)$ is the set described by (1) except that the X_i are taken from $\mathfrak{h} \otimes_k \Lambda$. To get this isomorphism of schemes, one must make the assumption that the exponential of any p-nilpotent $X \in \mathfrak{h} \otimes_k \Lambda$ lies in $H(\Lambda)$ for each Λ. A look at the proof in [SFB97a] shows that we still get an isomorphism of varieties with our weaker assumption.

If (ρ, V) satisfies the hypothesis of the lemma, we say that it is an exponential-type representation of H.

9.5. Let now G be a connected, semisimple, algebraic group over k. Let $\mathcal{N}_p = \mathcal{N}_p(\mathfrak{g})$, $\mathcal{N}_p(d) = \mathcal{N}_p(d, \mathfrak{g})$, and $\mathcal{A}(d) = \mathcal{A}(d, G)$.

The group G is determined up to isogeny by its root system R. Let r denote the rank of G. When G is quasisimple, R is either of classical type (hence is one of A_r, B_r, C_r, or D_r), or R is of exceptional type (hence is one of E_6, E_7, E_8, F_4 or G_2).

Theorem. *Let G be semisimple. Then $\mathcal{N}_p(d) \simeq \mathcal{A}(d)$ as G-varieties in each of the following cases:*

1. *$p > 2h - 2$ where h is the Coxeter number.*
2. *G is quasisimple and R is of classical type, and moreover $p \neq 2$ if $R = B_r, C_r, D_r$, and $r \not\equiv -1 \pmod{p}$ if $R = A_r$.*
3. *G is quasisimple and R is of exceptional type, and moreover $p \geq p_0$ where p_0 is given in the following table:*

R	p_0	R	p_0
G_2	7	E_6	17
F_4	17	E_7	29
		E_8	59

Proof. In all three cases, the condition on p guarantees that it does not divide the order of the fundamental group (this is well-known, and may be checked by looking at the tables in [Bou72]). So it suffices by Corollary 9.3, Lemma 9.4 and Proposition 9.4 to show that there is a semisimple group G' isogenous to G, and an exponential-type representation (ρ, V) of G'.

In case (1), this follows from Corollary 7.4 together with Remark 7.4(1).

In case (2), this follows from [SFB97a, Lemma 1.8].

In case (3), we get the result again by Corollary 7.4 together with Remark 7.4(2). □

9.6. Let G be connected and reductive, and let $P \leq G$ be a parabolic subgroup with unipotent radical $\mathrm{V} \leq P$ and $\mathfrak{v} = \mathrm{Lie}(\mathrm{V})$. Let $n(P)$ be the integer defined as in 4.4; this coincides with the nilpotence class of V and $\mathfrak{v}$ provided p is good; in particular, it coincides with the nilpotence class of $\mathrm{V}_{\mathbb{Q}}$ and $\mathfrak{v}_{\mathbb{Q}}$ as in section 8. The following is related to the question posed in [SFB97a, Remark 1.9] (see the discussion in the introduction).

Theorem. *Assume that $n(P) < p$. Then there is an injective morphism of P-varieties*

$$\varepsilon : \mathcal{N}_p(d, \mathfrak{v}) \to \mathcal{A}(d, \mathrm{V}).$$

Remark. The point of the theorem is that ε does not depend on the choice of a faithful representation of G.

Proof. In this case, we must first work with schemes in order to know that the map we define is a morphism.

Recall from Corollary 8 that there is an isomorphism of group schemes $\varepsilon : \mathfrak{v} \to \mathrm{V}$. Thus for each k-algebra Λ, each $X \in \mathfrak{v} \otimes_k \Lambda$ determines a homomorphism $\varepsilon_X : \mathbb{G}_{a,\Lambda} \to \mathrm{V}_\Lambda$. If $\vec{X} = (X_0, X_1, \dots, X_{d-1}) \in \underline{\mathcal{N}}(d, \mathfrak{v})(\Lambda)$, one emulates the construction in [SFB97a, Remark 1.3] to obtain a homomorphism of group schemes $\varepsilon_{\vec{X}} : \mathbb{G}_{a,\Lambda} \to \mathrm{V}_\Lambda$ (note that we must use here (2) of Corollary 8), and hence (by "restriction") a homomorphism of group schemes $\varepsilon_{\vec{X}} : \mathbb{G}_{a,d,\Lambda} \to \mathrm{V}_\Lambda$.

It is now easy to see that the assignment $\vec{X} \mapsto \varepsilon_{\vec{X}}$ is functorial in Λ, hence defines a morphism of schemes $\underline{\mathcal{N}}(d, \mathfrak{v}) \to \underline{\mathcal{A}}(d, V)$. We get then also a morphism of varieties $\mathcal{N}(d, \mathfrak{v}) \to \mathcal{A}(d, V)$; P-equivariance follows from (1) of Corollary 8.

To prove injectivity, we essentially copy the proof of [SFB97a, Lemma 1.7]. Suppose that $\varepsilon_{\vec{X}} = \varepsilon_{\vec{Y}}$. Differentiating gives then $X_0 = Y_0$. Multiplying each homomorphism with ε_{-X_0}, one sees that $\varepsilon_{(0,X_1,\dots,X_{d-1})} = \varepsilon_{(0,Y_1,\dots,Y_{d-1})}$ are equal. But then $\varepsilon_{(X_1,\dots,X_{d-1})}$ and $\varepsilon_{(Y_1,\dots,Y_{d-1})}$ coincide in $\mathcal{A}(d-1, V)$, and the injectivity of ε follows by induction (note that ε is an isomorphism of varieties when $d = 1$; see [SFB97a, Lemma 1.6]). □

9.7. Let H be a linear algebraic group over k. We recall briefly the significance of the variety $\mathcal{A}(d, H)$ for the cohomology of H_d. In the papers [SFB97a] and [SFB97b], Suslin, Friedlander and Bendel define a ring homomorphism

$$\Phi : H^{\text{even}}(H_d, k) \to k[\underline{\mathcal{A}}(d, H)],$$

and they show that the map induced by Φ on the corresponding schemes is a topological homeomorphism; clearly the same is still true after replacing $\underline{\mathcal{A}}(d, H)$ with $\mathcal{A}(d, H)$.

Now consider a connected reductive group G over k. It was shown by Friedlander and Parshall that for sufficiently large p, the cohomology $H^i(G_1, k)$ vanishes for i odd, and that the even cohomology ring $H^{\text{even}}(G_1, k)$ may be identified with the graded coordinate ring of $\mathcal{N}(\mathfrak{g})$. See also [AJ84], where it is proved that $p > h$ is sufficient. The proof of this fact in *loc. cit.* relies on knowledge of the dimensions of the homogeneous parts of $k[\mathcal{N}(\mathfrak{g})]$; thus it seems likely that further understanding of the cohomology of G_d might benefit from some understanding of $\mathcal{N}_p(d, \mathfrak{g})$. We conclude the paper with the following, in the hope that it might be useful (compare [AJ84, 3.9]).

Proposition. *If p is a good prime for G, there is an injective homomorphism of G-modules*

$$k[\mathcal{N}_p(d, \mathfrak{g})] \to H^0(G/B, k[\mathcal{N}_p(d, \mathfrak{u})]).$$

Proof. We mimic the argument in [AJ84]. Let $X = \bigoplus_{i=0}^{d-1} \mathfrak{g}^{[i]}$ (where the exponent $[i]$ denotes the i-th Frobenius twist); G acts on X by $\alpha = \bigoplus \mathrm{Ad}^{[i]}$. We denote also by α the action of G on the algebra $k[X]$ of regular functions on X. There is a homomorphism

$$k[X] \to H^0(G/B, k[\mathcal{N}_p(d, \mathfrak{u})])$$

obtained by mapping $f \in k[X]$ to the section $g \mapsto \big(\alpha(g^{-1})f\big)_{|\mathcal{N}_p(d,\mathfrak{u})}$. The kernel is

$$\{f \in k[X] \mid f \text{ vanishes on } \alpha(g)\mathcal{N}_p(d, \mathfrak{u}) \text{ for all } g \in G\},$$

and we claim this is the vanishing ideal of $\mathcal{N}_p(d, \mathfrak{g})$. It suffices to see that if $\{X_i\}$ is a set of pairwise commuting nilpotent elements in $\mathfrak{g}$, then the Abelian Lie algebra $\mathfrak{a}$ which they span is contained in a Borel subalgebra; that is a consequence of the lemma which follows. □

Lemma. *Suppose that p is good for G, and that B is a Borel subgroup of G with unipotent radical U. Let $\mathfrak{a} \subset \mathfrak{g}$ be an Abelian subalgebra generated by nilpotent elements. Then there is $g \in G$ such that* $\mathrm{Ad}(g)\mathfrak{a} \subset \mathfrak{u} = \mathrm{Lie}(U)$.

Proof. There is a central isogeny $G' \to G$ where G' is a direct product of a torus and quasisimple groups satisfying the hypothesis of Proposition 5.2. This isogeny induces a bijection (not in general an isomorphism of varieties) on the nilpotent sets in the respective Lie algebras. Thus, we may replace G with G', so that we may apply the results of [Spa84].

The result is well known if $\dim \mathfrak{a} = 1$. So now suppose that $\dim \mathfrak{a} > 1$, and let $0 \neq X \in \mathfrak{a}$. By the Theorem proved in [Spa84], there is a proper parabolic subgroup P of G with Levi decomposition $P = \mathrm{LV}$ such that $X \in \mathfrak{v} = \mathrm{Lie}(\mathrm{V})$ and $\mathfrak{c}_{\mathfrak{g}}(X) \subset \mathfrak{p} = \mathrm{Lie}(P)$ [in general, X need not be a Richardson element in $\mathfrak{v}$]. Thus, we have $\mathfrak{a} \subset \mathfrak{c}_{\mathfrak{g}}(X) \subset \mathfrak{p}$. Since $X \in \mathfrak{v}$, the image of $\mathfrak{a}$ in $\mathfrak{p}/\mathfrak{v}$ has dimension strictly less than that of $\mathfrak{a}$. We obtain by induction on $\dim \mathfrak{a}$ some $g \in \mathrm{L}$ such that the image of $\mathfrak{a}$ in $\mathfrak{l} \simeq \mathfrak{p}/\mathfrak{n}_{\mathfrak{p}}$ is conjugate via $\mathrm{Ad}(g)$ to a subalgebra of a Borel subalgebra of $\mathfrak{l}$. Since L leaves $\mathfrak{v}$ invariant, $\mathrm{Ad}(g)(\mathfrak{a})$ is contained in a Borel subalgebra of $\mathfrak{p}$ (which is in turn a Borel subalgebra of $\mathfrak{g}$). Since all Borel subalgebras of $\mathfrak{g}$ are conjugate, we obtain the lemma. □

References

[AJ84] Henning H. Andersen and Jens C. Jantzen, *Cohomology of induced representations for algebraic groups*, Math. Ann. **269** (1984), 487–525.

[BC76a] P. Bala and R. W. Carter, *Classes of unipotent elements in simple algebraic groups. I*, Math. Proc. Cambridge Philos. Soc. **79** (1976), no. 3, 401–425.

[BC76b] P. Bala and R. W. Carter, *Classes of unipotent elements in simple algebraic groups. II*, Math. Proc. Cambridge Philos. Soc. **80** (1976), no. 1, 1–17.

[Bor70] Armand Borel, *Properties and linear representations of Chevalley groups*, Seminar on Algebraic Groups and Related Finite Groups (The Institute for Advanced Study, Princeton, N.J., 1968/69), Springer, Berlin, 1970, Lecture Notes in Mathematics, Vol. 131, pp. 1–55.

[Bor91] Armand Borel, *Linear algebraic groups*, 2nd ed., Grad. Texts in Math., no. 129, Springer Verlag, 1991.

[Bou72] N. Bourbaki, *Groupes et algèbres de Lie, chapitres 4,5,6*, Hermann, Paris, 1972.

[Bou89] N. Bourbaki, *Lie groups and Lie algebras, chapters 1,2,3*, Springer-Verlag, Berlin, 1989.

[BT73] Armand Borel and Jacques Tits, *Homomorphismes "abstraits" de groupes algébriques simples*, Ann. of Math. (2) **97** (1973), 499–571.

[Car93] Roger W. Carter, *Finite groups of Lie type*, John Wiley & Sons Ltd., Chichester, 1993, Conjugacy classes and complex characters, Reprint of the 1985 original, A Wiley-Interscience Publication.

[GLMS97] Robert M. Guralnick, Martin W. Liebeck, Dugald Macpherson, and Gary M. Seitz, *Modules for algebraic groups with finitely many orbits on subspaces*, J. Algebra **196** (1997), no. 1, 211–250.

[Hal76] Marshall Hall, Jr., *The theory of groups*, Chelsea Publishing Co., New York, 1976, Reprinting of the 1968 edition.

[Hum95] James E. Humphreys, *Conjugacy classes in semisimple algebraic groups*, Math. Surveys and Monographs, vol. 43, Amer. Math. Soc., 1995.

[Jac62] Nathan Jacobson, *Lie algebras*, Interscience Publishers (a division of John Wiley & Sons), New York-London, 1962.

[Jan87] Jens C. Jantzen, *Representations of algebraic groups*, Pure and Applied Mathematics, vol. 131, Academic Press, Orlando, FL, 1987.

[Kob77] Neal Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, Vol. 58.

[Pom77] Klaus Pommerening, *Über die unipotenten Klassen reduktiver Gruppen*, J. Algebra **49** (1977), no. 2, 525–536.

[Pom80] Klaus Pommerening, *Über die unipotenten Klassen reduktiver Gruppen. II*, J. Algebra **65** (1980), no. 2, 373–398.

[Pre95] Alexander Premet, *An analogue of the Jacobson-Morozov theorem for Lie algebras of reductive groups of good characteristics*, Trans. Amer. Math. Soc. **347** (1995), no. 8, 2961–2988.

[Pro] Richard Proud, *Witt groups and unipotent elements in algebraic groups*, Proc. Amer. Math. Soc., to appear.

[Ree57] Rimhak Ree, *On some simple groups defined by C. Chevalley*, Trans. Amer. Math. Soc. **84** (1957), 392–400.

[Sei00] Gary M. Seitz, *Unipotent elements, tilting modules, and saturation*, Invent. Math **141** (2000), 467–502.

[Ser79] Jean-Pierre Serre, *Local fields*, Grad. Texts in Math., vol. 67, Springer Verlag, 1979.

[Ser88] Jean-Pierre Serre, *Algebraic groups and class fields*, Grad. Texts in Math., no. 117, Springer-Verlag, New York, 1988.

[Ser96] Jean-Pierre Serre, *Exemples de plongements des groupes $PSL_2(\mathbf{F}_p)$ dans des groupes de Lie simples*, Invent. Math. **124** (1996), no. 1-3, 525–562.

[SFB97a] Andrei Suslin, Eric M. Friedlander, and Christopher P. Bendel, *Infinitesimal 1-parameter subgroups and cohomology*, J. Amer. Math. Soc. **10** (1997), no. 3, 693–728.

[SFB97b] Andrei Suslin, Eric M. Friedlander, and Christopher P. Bendel, *Support varieties for infinitesimal group schemes*, J. Amer. Math. Soc. **10** (1997), no. 3, 729–759.

[Spa84] Nicolas Spaltenstein, *Existence of good transversal slices to nilpotent orbits in good characteristic*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **31** (1984), no. 2, 283–286.

[Spr69] Tonny A. Springer, *The unipotent variety of a semi-simple group*, Algebraic Geometry (Internat. Colloq., Tata Inst. Fund. Res., Bombay, 1968), Oxford Univ. Press, London, 1969, pp. 373–391.

[Spr98] Tonny A. Springer, *Linear algebraic groups*, 2nd ed., Progr. in Math., vol. 9, Birkhäuser, Boston, 1998.

[SS70] Tonny A. Springer and Robert Steinberg, *Conjugacy classes*, Seminar on Algebraic Groups and Related Finite Groups (The Institute for Advanced Study, Princeton, N.J., 1968/69), Springer, Berlin, 1970, Lecture Notes in Mathematics, Vol. 131, pp. 167–266.

[Ste68] Robert Steinberg, *Lectures on Chevalley groups*, Yale University, 1968.

[Tes95] Donna Testerman, *A_1-type overgroups of elements of order p in semisimple algebraic groups and the associated finite groups*, J. Algebra **177** (1995), 34–76.

E-mail address: `mcninchg@member.ams.org`