Università degli Studi di Torino · Scuola di Scienze della Natura

Corso di Laurea Magistrale in Matematica
Master of Science in Mathematics

Unipotent algebraic groups over arbitrary fields

Matilde Maccan · 843092

Relatore: *Cinzia Casagrande*
Corelatore: *Matthieu Romagny*

Controrelatore: *Andrea Mori*

Anno accademico 2020/2021 · 15 luglio 2021

Contents

Introduction

The aim of this Master Thesis is to introduce and study unipotent algebraic group schemes over a perfect or imperfect ground field.

The first chapter begins with the definition of unipotency, proves that such groups naturally identify as subgroups of unipotent upper triangular matrices and deduces some fundamental properties.
The second chapter covers the theory of commutative unipotent algebraic groups over a perfect field, having as aim to establish an equivalence of categories between them and the so called Dieudonné modules.
Then, the texts proceeds further on with a brief discussion of the motivations leading to the study of the theory of unipotent groups over arbitrary fields of nonzero characteristic, mainly developed by J. Tits in the 1960's. In particular, the following very recent rigidity result by Z. Rosengarten (to appear, 2021) is mentioned.

Theorem 1 (Rosengarten)**.** *Let G and H be group schemes of finite type over a field k of degree of imperfection* 1*. Assume that G is unirational and that H is solvable and does not contain a k-subgroup isomorphic to $\mathbb{G}_a$. Then any k-scheme morphism $f\colon G \longrightarrow H$ such that $f(1_G) = 1_H$ is a homomorphism of k-group schemes.*

Finally, the last chapter develops Tits' theory in detail, from a preliminary study of subgroups of vector groups, to the definition of the wound property, concluding with a result of triviality of actions by tori on such groups:

Theorem 2. *Let T be a k-torus and U a smooth connected unipotent algebraic group over k. If U is k-wound, the only T-action on U is the trivial one.*

I would like to thank my supervisor Matthieu Romagny for all the help and advice he has given me during my first year in France.

Notations

Throughout this text, k denotes a field, which starting from the second chapter is assumed to be of nonzero characteristic, and R denotes a commutative k-algebra. Given a field k, an algebraic closure $\overline{k}$ is fixed and k_s denotes the separable closure inside of $\overline{k}$. Whenever it is not specified, tensor products are to be considered over the base field k; analogously, fiber products are to be considered over $\operatorname{Spec} k$.
An **algebraic group** over k, or a **k-group** is a group scheme of finite type over k, and all algebraic groups are to be considered **affine**. All constructions are to be included in the setting of scheme theory : the Yoneda lemma is often used in order to describe a group scheme or a scheme in terms of its functor of points and to work respectively with abstract groups or sets.

Comparison with the reductive case

In order to introduce the topic properly, it is natural to highlight the role of unipotent groups among algebraic group schemes over a field : in particular, we compare two orthogonal families of groups, reductive and unipotent ones. More precisely, orthogonal is intended in the sense of the following result: over an algebraically closed field k, any smooth connected k-group G fits in an exact sequence of the form

$$1 \longrightarrow R_{u,k}(G) \longrightarrow G \longrightarrow G/R_{u,k}(G) \longrightarrow 1,$$

where $R_{u,k}(G)$ denotes its unipotent radical and the quotient $G/R_{u,k}(G)$ is a reductive group i.e. does not contain any smooth connected unipotent normal k-subgroup.

Reductive groups "behave very well": their structure is known and has been studied extensively, while unipotent groups are harder to understand and classify. First, let us list, without proofs, a few results that highlight the many differences between these two classes; next, we discuss a bit more in detail the representability of the respective moduli spaces.

	REDUCTIVE	**UNIPOTENT**
Unirationality	Yes	Not in general
Rational points	Form an open, Zariski-dense subscheme	Can be reduced to 1
Picard group	Finite	Can be infinite
Automorphism group	Represented by an algebraic group	Not algebraic

Moduli spaces

Let us consider a smooth connected k-group G and a property $\mathbf{P}$ of group schemes. Define the functor $F_{\mathbf{P}}$ classyfying subgroups of G having property $\mathbf{P}$ as follows:

$$F_{\mathbb{P}}\colon (\mathrm{k}-\mathbf{Alg}) \longrightarrow (\mathbf{Grp}),$$
$$R \longmapsto F_{\mathbf{P}}(R) := \{ \text{ smooth connected } R\text{-subgroups of } G_R \text{ having property } \mathbf{P} \}.$$

Looking at reductivity, the corresponding functor is representable by a k-scheme. Conversely, taking as $\mathbf{P}$ the property of being unipotent, it is not representable in general : let k be a field of characteristic 0 and consider the k-group $G = \mathbb{G}_a \times \mathbb{G}_m$. For any k-scheme X,

$$X(k[\![T]\!]) = \varprojlim_{n\in\mathbb{N}} X\left(k[T]/T^{n+1}\right),$$

which gives a necessary condition for the representability of a functor, called the **effectivity of formal deformations**. This is due to the fact that $k[\![T]\!]$ is a local ring and that for a local ring A, there is a bijection

$$\mathrm{Hom}_{(\mathrm{k}-\mathbf{Sch})}(\mathrm{Spec}\, A, X) \simeq \{(x,\varphi)\colon x \in X,\ \varphi\colon \mathcal{O}_{X,x} \to A \text{ a local morphism } \}.$$

However, we claim that

$$F(k[\![T]\!]) \longrightarrow \varprojlim_{n\in\mathbb{N}} F\left(k[T]/T^{n+1}\right)$$

is not a bijection, hence F cannot be representable. To see this, let $P_n \in \left(k[T]/T^{n+1}\right)[X]$ be the polynomial

$$P_n(X) := 1 + TX + \frac{TX^2}{2} + \ldots + \frac{T^nX^n}{n!},$$

so that its graph $H_n \subset G_{k[T]/T^{n+1}}$ is isomorphic to the additive group $\mathbb{G}_{a,k[T]/T^{n+1}}$ so it is smooth connected and unipotent, hence it can be seen as an element of $F\left(k[T/T^{n+1}\right)$. Moreover, the collection $(P_n)_{n\in\mathbb{N}}$ is compatible with projections, so it defines an element of the projective limit. However, this element does not have any preimage in $F(k[\![T]\!])$, because there exists no $P \in k[\![T]\!][X]$ such that $P_{|k[T]/T^{n+1}} = P_n$.

Groundwork on unipotent groups

This chapter is dedicated to illustrating in detail the definition of unipotent algebraic groups and some of their fundamental properties. The reader will be assumed to be familiar with basic algebraic geometry, for which the main reference is [GW]. Most fundamental results from the theory of algebraic groups over fields, such as their definition, the existence of quotients, several properties of tori and groups of multiplicative type, will be often used without explicitly stating nor proving them. With respect to these topics, the main references are [Bor91] for what concerns the classical theory (without modern algebraic geometry methods and working over an algebraically closed field) and the first 12 chapters of [Mil17] for the group scheme point of view.

1.1 Definition

1.1.1 Preliminaries

To better understand the definition of unipotent algebraic groups, which is given in terms of their representations, we shall give some preliminaries on linear representations, in particular on the subspace of a vector space V fixed by a k-group acting on it.

Recall that a representation of G on a vector space V can be regarded as a morphism of group-valued functors $r\colon G \to \mathrm{GL}_V$: it is given by a the collection of group morphisms

$$r_R\colon G(R) \to \mathrm{GL}_V(R) = \mathrm{Aut}_k(V \otimes R)$$

for all k-algebras R, functorial in R. To simplify notations, for $g \in G(R)$ and $w \in V \otimes R$, we will denote $g \cdot w$ instead of $r_R(g)(w)$.

Definition 1.1.1. Let G be an algebraic group over k and (V, r) a representation of G. The subspace fixed by G is

$$V^G := \{v \in V\colon g \cdot (v \otimes 1) = v \otimes 1 \in V \otimes R, \text{ for all } k\text{-algebras } R \text{ and all } g \in G(R)\}.$$

Since we will often be interested in working in functorial terms, it is useful to understand the structure of the vector group associated to this subspace, which is the functor $R \mapsto V^G \otimes R$.

Proposition 1.1.2. *Let R be a k-algebra and (V, r) a representation of an algebraic group G. Then*

$$V^G \otimes R = \{w \in V \otimes R\colon g \cdot w = w \text{ for all } g \in G(R'), \text{ for all } R\text{-algebras } R'\}.$$

Proof. Let $w \in V \otimes R$ a vector satisfying the above condition. Let us fix $(e_i)_{i \in I}$ a basis of R as a k-vector space, and write $w = \sum_{i \in I} v_i e_i$ for some $v_i \in V$. To conclude that $w \in V^G \otimes R$, it suffices to prove that all v_i belong to V^G. Let S be a k-algebra and $g \in G(S)$: by definition of V^G, we need to prove that $g(v_i \otimes 1) = v_i \otimes 1$. Let us take as R' the R-algebra $S \otimes R$. Consider the canonical k-algebra morphism

$S \to S \otimes R$ sending s to $s \otimes 1$, which induces a morphism $G(S) \to G(S \otimes R)$. Let g' be the image of g under this morphism. By hypothesis, $\sum_{i \in I} v_i \otimes 1 \otimes e_i$ is fixed by g', so we have

$$\sum_{i \in I} v_i \otimes 1 \otimes e_i = g'(\sum_{i \in I} v_i \otimes 1 \otimes e_i) = \sum_{i \in I} g(v_i \otimes 1) \otimes e_i,$$

and since the e_i form a basis, we conclude that $g(v_i \otimes 1) = v_i \otimes 1$. □

Corollary 1.1.3. *Let G be an algebraic group over k, (V, r) a representation of G and N a normal algebraic subgroup. Then V^N is stable under G.*

Proof. Let R be a k-algebra, $v \in V^N \otimes R$ and $g \in G(R)$, our aim is to prove that $g \cdot v$ is still in $V^N \otimes R$. By 1.1.2,

$$V^N \otimes R = \{w \in V \otimes R \colon n \cdot w = w \text{ for all } n \in N(R'), \text{ for all } R\text{-algebras } R'\}.$$

Let R' be an R-algebra and $n \in N(R')$ and denote $v_{R'}$ the image of v by the morphism $R \to R'$: then

$$n \cdot (g \cdot v)_{R'} = (ng) \cdot v_{R'} = (gn') \cdot v_{R'} = g \cdot (n' \cdot v_{R'}) = g \cdot v,$$

because $n' = g^{-1}ng$ is in $N(R')$ hence fixes $v_{R'}$. □

The following proposition reformulates the definition of V^G in terms of the associated comodule, which allows us to easily prove that the formation of V^G commutes with extension of the base field.

Proposition 1.1.4. *Let (V, r) be a representation of an algebraic group G and denote $\rho \colon V \to V \otimes \mathcal{O}(G)$ the associated $\mathcal{O}(G)$-comodule. Then*

$$V^G = \{v \in V \colon \rho(v) = v \otimes 1 \in V \otimes \mathcal{O}(G)\}. \tag{1.1}$$

Proof. This follows from the correspondence between linear representations of G and $\mathcal{O}(G)$-comodules: see [Mil17, 4.a]. □

Corollary 1.1.5. *Let k'/k be a field extension and $r \colon G \to \mathrm{GL}_V$ a representation of a k-group G. Then $r_{k'} \colon G_{k'} \to GL_{V \otimes k'}$ is a representation of $G_{k'}$ on the vector space $V \otimes k'$, satisfying*

$$(V \otimes k')^{G_{k'}} \simeq V^G \otimes k'.$$

Proof. The condition 1.1 is k-linear, hence it commutes with a field extension of k. □

1.1.2 Definition in terms of representations

Definition 1.1.6. An algebraic group G over k is said to be **unipotent** if every nonzero representation of G has a nonzero fixed vector.

This definition is equivalent to saying that its only irreducible representations are one-dimensional vector spaces equipped with a trivial action of G. If we denote $\rho \colon V \to V \otimes \mathcal{O}(G)$ the comodule associated to any representation (V, r) of G, the definition of unipotent group is equivalent to the existence of a nonzero vector $v \in V$ such that $\rho(v) = v \otimes 1$. Moreover, since every representation is a directed union of its finite-dimensional subrepresentations ([Mil17], Corollary 4.8), it suffices to check its existence only for V finite-dimensional. Let us recall some basics notations : the general linear group GL_n is given as a functor by $(\mathrm{k}-\mathbf{Alg}) \to (\mathbf{Grp})$, $R \mapsto \mathrm{GL}_n(R)$, where $\mathrm{GL}_n(R)$ denotes the invertible matrices of order n having entries in the k-algebra R. Its coordinate ring is

$$\mathcal{O}(\mathrm{GL}_n) = k[X_{11}, X_{12}, \dots, X_{nn}, 1/\det(X_{ij})]$$

and the comultiplication map is given by

$$\Delta(X_{ij}) = \sum_{h=1}^{n} X_{ih} \otimes X_{hj}.$$

The algebraic group $\mathbb{U}_n$ is the subgroup of GL_n whose functor of points is

$$\mathbb{U}_n \colon (\mathrm{k}-\mathbf{Alg}) \to (\mathbf{Grp}), \quad R \mapsto \mathbb{U}_n(R) := \{(a_{ij}) \in \mathrm{GL}_n(R) \colon a_{ij} = 0 \text{ for } i > j, a_{ij} = 1 \text{ for } i = j\},$$

i.e. the matrices of the form

$$\begin{pmatrix} 1 & * & * & \cdots & * \\ & 1 & * & & * \\ & & \ddots & \ddots & \vdots \\ & 0 & & 1 & * \\ & & & & 1 \end{pmatrix}$$

Its coordinate ring is the quotient of $\mathcal{O}(\mathrm{GL}_n)$ by the ideal generated by the polynomials X_{ij} for $i > j$ and $X_{ii} - 1$, while the comultiplication comes from the one in GL_n:

$$\mathcal{O}(\mathbb{U}_n) = k[X_{ij}, i < j], \quad \Delta(X_{ij}) = X_{ij} \otimes 1 + 1 \otimes X_{ij} + \sum_{i<h<j} X_{ih} \otimes X_{hj}. \tag{1.2}$$

Definition 1.1.7. A finite-dimensional representation (V, r) of an algebraic group G is a **unipotent representation** if there exists a basis of V such that $r(G) \subset \mathbb{U}_n$.

Proposition 1.1.8. *An algebraic group G is unipotent if and only if every finite-dimensional representation of G is a unipotent representation.*

Proof. Let us fix a finite-dimensional representation (V, r) of G: by definition of $\mathbb{U}_n$, r is unipotent if and only if there exist vector subspaces $V = V_s \supset \cdots \supset V_1 \supset 0$ such that each V_i is stable under the action of G and this action is trivial on each of the successive quotients V_{i+1}/V_i. Let G be unipotent and fix a composition series for V, i.e. a maximal subnormal series of V when seen as a G-module. By maximality, each successive quotient must be simple, thus G acts trivially on it. The representation is hence unipotent. Conversely, suppose that all finite-dimensional representations (V, r) are unipotent: fix V and consider such a flag $V = V_s \supset \cdots \supset V_1 \supset 0$ assuming that V_1 is nonzero. Since G acts trivially on it, there exists a nonzero fixed vector in V, hence by definition G is unipotent. □

1.1.3 Embedding in $\mathbb{U}_n$

The aim of this pararaph is to prove that, for an algebraic group G, being unipotent is equivalent to admitting an embedding in $\mathbb{U}_n$ for some n. To prove this, one needs to introduce a technical definition concerning Hopf algebras. Let us recall that a k-scheme of finite type $G = \operatorname{Spec} A$ is an algebraic group G if and only if A is a finitely generated Hopf algebra, i.e. it admits k-algebra homomorphisms $\Delta\colon A \to A \otimes A$ (**comultiplication**), $\epsilon\colon A \to k$ (**counit**) and $S\colon A \to A$ (**antipode**) satisfying the following diagrams:

$$\begin{array}{ccc} A \otimes A \otimes A & \xleftarrow[\mathrm{id} \otimes \Delta]{} & A \otimes A \\ {\scriptstyle \Delta \otimes \mathrm{id}} \uparrow & & \uparrow {\scriptstyle \Delta} \\ A \otimes A & \xleftarrow[\Delta]{} & A \end{array}$$

$$\begin{array}{ccccc} k \otimes A & \xleftarrow[\epsilon \otimes \mathrm{id}]{} & A \otimes A & \xrightarrow{\mathrm{id} \otimes \epsilon} & A \otimes k \\ & \nwarrow & {\scriptstyle \Delta} \uparrow & \nearrow & \\ & & A & & \end{array}$$

$$\begin{array}{ccccc} A & \xleftarrow[S \cdot \mathrm{id}]{} & A \otimes A & \xrightarrow{\mathrm{id} \cdot S} & A \\ \uparrow & & {\scriptstyle \Delta} \uparrow & & \uparrow \\ k & \xleftarrow[\epsilon]{} & A & \xrightarrow{\epsilon} & k \end{array}$$

All properties and maps of Hopf algebras can be translated into geometric terms: for instance, the comultiplication, counit and antipode in $\mathcal{O}(G)$ correspond to the multiplication, unity and inversion maps in G. These are easier to understand intuitively but sometimes harder to manipulate than their algebraic counterpart.

Definition 1.1.9. Let A be a k-algebra. A **filtration** of A is an increasing sequence of vector subspaces $(F_i)_{i \in \mathbb{N}}$ such that

- $1 \in F_0$,
- $\bigcup_{i \in \mathbb{N}} F_i = A$,
- $F_i F_j \subseteq F_{i+j}$ for all i, j.

Definition 1.1.10. A k-Hopf algebra $A = (A, \Delta, \epsilon, S)$ is said to be **coconnected** is there exists a filtration $C_0 \subset C_1 \subset C_2 \subset \cdots$ of A such that

$$C_0 = k \quad \text{and} \quad \Delta(C_r) \subset \sum_{i=0}^{r} C_i \otimes C_{r-i} \text{ for all } r \in \mathbb{N}.$$

Theorem 1.1.11 (Characterisation of unipotent groups)**.** *Let G be an algebraic group over k. The following assertions are equivalent:*

(1) G is unipotent.

*(2) There exists an integer n such that G is isomorphic to an algebraic **subgroup of** $\mathbb{U}_n$.*

(3) The Hopf algebra $\mathcal{O}(G)$ is coconnected.

In other words, the equivalence between (1) and (2) means that an algebraic group is unipotent if and only if it admits a faithful unipotent representation.

Proof. (1) ⇒ (2) : Suppose G is unipotent, and consider a faithful finite dimensional representation of G, i.e. a closed immersion $G \hookrightarrow \mathrm{GL}_n$. By Proposition 1.1.8, this representation is unipotent : up to a base change in $V = k^n$, it factorizes as $G \hookrightarrow \mathbb{U}_n \hookrightarrow \mathrm{GL}_n$.
(2) ⇒ (3) : Let G be a k-subgroup of $\mathbb{U}_n$: since all monomorphisms of algebraic groups are closed immersions, this corresponds to the Hopf algebra $\mathcal{O}(G)$ being a quotient of $\mathcal{O}(\mathbb{U}_n)$ by a Hopf ideal I. First, let us prove that every quotient of a coconnected Hopf algebra is coconnected. Let A be a coconnected Hopf algebra, I a Hopf ideal and consider the quotient $\pi\colon A \twoheadrightarrow A/I =: B$. Fix a filtration $(C_r)_{r\geqslant 0}$ of A satisfying the definition 1.1.10. Then $D_r := \pi(C_r)$ is the desired filtration for B, because

- π is a k-algebra morphism, hence $D_0 = \pi(C_0) = \pi(k) = k$,
- $\sum_{r\geqslant 0} D_r = \sum_{r\geqslant 0} \pi(C_r) = \pi(A) = B$,
- π is a k-coalgebra morphism, hence

$$\begin{aligned}\Delta_B(D_r) =& \Delta_B \circ \pi(C_r) = (\pi\otimes\pi)\circ\Delta_A(C_r) \subset (\pi\otimes\pi)\left(\sum_{i=0}^{r} C_i \otimes C_{r-i}\right)\\ =& \sum_{i=0}^{r}(\pi\otimes\pi)(C_i\otimes C_{r-i}) = \sum_{i=0}^{r} D_i\otimes D_{r-i}.\end{aligned}$$

By (2), this implies that it suffices to prove that $\mathcal{O}(\mathbb{U}_n) = k[X_{ij}, i<j]$ is coconnected. For this, let us assign to each monomial X_{ij} a weight $j-i$, and extend this to $X_{ij}^{n_{ij}}$ having weight $n_{ij}(j-i)$ and to any monomial $\prod X_{ij}^{n_{ij}}$ having weight $\sum_{i,j} n_{ij}(j-i)$. Now define C_r as being the vector subspace of $\mathcal{O}(\mathbb{U}_n)$ spanned by the monomials of weight less or equal to r. Clearly $C_0 = k$ and A is the union of the C_r. Moreover, if two monomials P and Q have weights r and s respectively, then PQ has weight $r+s$. This implies that $C_rC_s \subseteq C_{r+s}$. Finally, we need to verify the condition on the comultiplication on monomials. Let us proceed by induction on the weight of a monomial: by 1.2, $\Delta X_{ij} \in C_{j-i}\otimes C_0 + C_0\otimes C_{j-i} + \sum_{i<h<l} C_{h-i}\otimes C_{j-h}$. If we assume the condition satisfied by monomials P, Q of weights r and s, then

$$\Delta(PQ) = \Delta(P)\Delta(Q) \in \left(\sum_{a=0}^{r} C_i\otimes C_{r-a}\right)\left(\sum_{b=0}^{s} C_b\otimes C_{s-b}\right) \subset \sum_{a,b} C_aC_b\otimes C_{r-a}C_{s-b} \subset \sum_{a,b} C_{a+b}\otimes C_{r+s-(a+b)}$$

hence the condition is also satisfied for monomials of weights $r+s$.
(3) ⇒ (1) : Let $A := \mathcal{O}(G)$ be coconnected with filtration $(C_r)_{r\geqslant 0}$ and consider a comodule $\rho\colon V \to V\otimes A$: we want to prove that the corresponding representation of G has a nonzero fixed vector. For all $r\in\mathbb{N}$, set

$$V_r := \{v\in V\colon \rho(v)\in V\otimes C_r\},$$

then V is the union of the V_r and $V_0 = V^G$ by Proposition 1.1.4. Thus, to conclude it suffices to show that $V_r = 0$ implies $V_{r+1} = 0$. Let $v\in V_{r+1}$, then by definition $\rho(v)$ belongs to $V\otimes C_{r+1}$. Using the definitions of comodule and of coconnected Hopf algebra, we obtain

$$\alpha(v) := (\rho\otimes\mathrm{id}_A)\circ p(v) = (\mathrm{id}_V\otimes\Delta)\circ\rho(v) \in V\otimes\left(\sum_{i=0}^{r+1} C_i\otimes C_{r+1-i}\right). \tag{1.3}$$

Now, if $V_r = 0$, then ρ gives an injective map $V \to V \otimes A/C_r$, hence α gives an injective map

$$V \longrightarrow (V \otimes A/C_r) \otimes A/C_r.$$

By 1.3, this sends V_{r+1} to zero, hence $V_{r+1} = 0$ and we are done. $\square$

Corollary 1.1.12. *(a) Subgroups, quotients and extensions of unipotent groups are unipotent.*

(b) Every algebraic group G over k contains a largest smooth connected unipotent normal subgroup: this is called the ***unipotent radical*** *of G and denoted $R_{u,k}(G)$.*

(c) Let G be an algebraic group over k and k'/k a field extension. Then G is unipotent if and only if $G_{k'}$ is unipotent.

Proof. (a) : Let G be unipotent and H a k-subgroup of G. By 1.1.11, there exists an embedding

$$H \hookrightarrow G \hookrightarrow \mathbb{U}_n$$

for some n, hence H is unipotent too. Let $Q = G/H$ be a quotient of G and denote $\pi\colon G \to Q$ the quotient map. Consider a representation of Q on a vector space V. By precomposing with the quotient map,

$$G \xrightarrow{\pi} Q \longrightarrow \mathrm{GL}_V$$

we obtain a representation of G, which has a nonzero fixed vector $v \in V$ because G is unipotent. Therefore, v is also fixed by Q and we conclude that Q is unipotent. Finally, let us consider an algebraic group G and a normal algebraic subgroup N such that both N and G/N are unipotent. Let $r\colon G \to \mathrm{GL}_V$ be a nonzero representation of G. By 1.1.3, V^N is stable under G, so we obtain a representation of G on V^N. Since it is an N-invariant morphism, by universal property of the quotient it induces an unique representation of G/N as shown in the following diagram:

$$\begin{array}{ccc} G & \xrightarrow{\quad r \quad} & \mathrm{GL}_{V^N} \\ & \searrow & \nearrow_{\exists !} \\ & G/N & \end{array}$$

Now, V is nonzero and N is unipotent, hence V^N is nonzero. Moreover, the equality $V^G = (V^N)^{G/N}$ and the unipotence of G/N imply that V^G is nonzero too. Hence G is unipotent as desired.
(b) : we use the following result, which is a consequence of the isomorphism theorems for algebraic groups (see [Mil17], Proposition 6.42) : let **P** be a property of algebraic groups such which is preserved by quotients and extensions. Then every algebraic group G contains a largest smooth connected subgroup H having property P. Moreover, the quotient G/H contains no nontrivial subgroup with property **P**. By (a), we can apply this proposition to the property **P** =unipotent and conclude the existence and uniqueness of the unipotent radical.
(c) : Let G be unipotent, by 1.1.11 the Hopf algebra $\mathcal{O}(G)$ is coconnected: let us denote its filtration as $(C_r)_{r\geqslant 0}$. By taking $(C_r \otimes k')_{r\geqslant 0}$ as a filtration of $\mathcal{O}(G) \otimes k'$ we see that it is coconnected too, hence $G_{k'}$ is unipotent. Conversely, assume $G_{k'}$ is unipotent and let (V, r) be a representation of G. Since

$G_{k'}$ is unipotent, $(V^G \otimes k')^{G_{k'}}$ is nonzero, while by 1.1.5 it is equal to $V^G \otimes k'$, so V^G is nonzero too and we are done. □

1.2 Basic properties

1.2.1 Unipotent groups and groups of multiplicative type

The notion of unipotent algebraic group is orthogonal to the notion of group of multiplicative type, in a sense that we will specify in the following section. Let us recall that an algebraic group over k is of multiplicative type if and only if it becomes diagonalizable over an algebraic closure $\bar{k}$, which is equivalent to being diagonalizable over some finite separable extension of the base field (see [Mil17, Ch. 12]).

Proposition 1.2.1. *An algebraic group that is both unipotent and of multiplicative type is trivial.*

Proof. Let G be such an algebraic group over k. Let us consider an embedding $G \hookrightarrow \mathrm{GL}_V$ for some finite-dimensional k-vector space V. By extending scalars to a suitable finite field extension k'/k, we can suppose G is both diagonalizable and unipotent, thanks to Corollary 1.1.12. Since an algebraic group is diagonalizable if and only if all its linear representations are diagonalizable, V is a direct sum of simple representations V_i. By unipotency of G, each of the V_i has a nonzero fixed vector, hence the action of G on it must be trivial. □

Corollary 1.2.2.

- *Let G be an algebraic group over k. The intersection of a unipotent k-subgroup with a k-subgroup of multiplicative type is trivial.*
- *Let U and M be algebraic groups over k which are respectively unipotent and of multiplicative type. Then*
$$Hom_{(\mathrm{k-\mathbf{Grp}})}(M,U) = 0 \quad \text{and} \quad Hom_{(\mathrm{k-\mathbf{Grp}})}(U,M) = 0.$$

Proof. Let U and M be such subgroups. Then their intersection is a k-subgroup of U, hence it is unipotent by 1.1.12. Moreover, the property of being of multiplicative type is also inherited by subgroups, so $U \cap M$ is trivial by 1.2.1.
Now, let us consider a k-homomorphism $\varphi\colon U \to M$. By the homomorphism theorem, we can factorize it as
$$\varphi\colon U \overset{q}{\twoheadrightarrow} U/\ker\varphi = \varphi(U) \overset{i}{\hookrightarrow} M,$$
with q faithfully flat and i a closed immersion. This shows that the image $\varphi(U)$ can be realized both as a quotient of U, which is unipotent by 1.1.12, and as a subgroup of M, which is of multiplicative type. Thus, we conclude that the morphism φ is trivial. The same proof works for any k-homomorphism $\psi\colon M \to U$. □

1.2.2 Nilpotence and composition series

Another significant property of unipotent algebraic groups is that they are nilpotent : in order to prove this, let us recall some terminology. A **subnormal series** for an algebraic group G over k is a finite sequence
$$G = G_0 \supset G_1 \supset \cdots \supset G_r = 1$$
of k-subgroups such that G_i is a normal subgroup of G_{i-1} for $i = 1, \ldots, r$. If each G_i is normal in G, it is called a **normal** series.

Definition 1.2.3. Let G be an algebraic group over k. A **composition series** is a subnormal series $(G_i)_{i=0}^r$ such that

$$\dim G_0 > \dim G_1 > \cdots > \dim G_r = 0$$

and which is maximal among subnormal series satisfying this property.

Finally, let us recall that an algebraic group is said to be :

- **solvable** if it admits a subnormal series whose successive quotients G_i/G_{i+1} are commutative, also called a solvable series;
- **nilpotent** if it admits a normal series such that each quotient G_i/G_{i+1} is contained in the center of G/G_{i+1}, also called a nilpotent series.

In other words, a solvable group can be obtained by successive extensions of commutative algebraic groups, while for a nilpotent group we can even assume those extensions to be central.

Lemma 1.2.4. *For any integer $n \geqslant 1$, the algebraic group $\mathbb{U}_n$ admits a central normal series whose successive quotients are isomorphic to $\mathbb{G}_a$.*

Proof. Let us fix an $n \in \mathbb{N}$ and consider the pairs (i,j) with $1 \leqslant i < j \leqslant n$, which we number as follows:

$$\begin{array}{ccccc} C_1 = (1,2) & C_2 = (2,3) & C_3 = (3,4) & \cdots & C_{n-1} = (n-1,n) \\ & C_n = (1,3) & C_{n+1} = (2,4) & \cdots & C_{2n-3} = (n-2,n) \\ & & & \cdots & \cdots \\ & & & & C_N = (1,n), \end{array}$$

with $N = n(n-1)/2$. For $s = 0, \dots, N$, let us denote as G_s the algebraic subgroup of $\mathbb{U}_n$ having as functor of points

$$G_s(R) := \{(a_{ij}) \in \mathbb{U}_n(R) \colon a_{ij} = 0 \text{ for } (i,j) = C_l, l \leqslant s\}.$$

We claim that the $(G_s)_{s=0}^N$ give a central normal series for $\mathbb{U}_n$. The case $n = 2$ is trivial, since $\mathbb{U}_2$ is already isomorphic to $\mathbb{G}_a$ and the second term of the series above is the neutral element. Let us prove our claim for $n = 3$ in order to simplify notations : in this case,

$$G_0 = \mathbb{U}_3 = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\}, \quad G_1 = \left\{ \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \right\}, \quad G_2 = \left\{ \begin{pmatrix} 1 & 0 & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}, \quad G_3 = 1.$$

With a straightforward calculation on the functor of points, one verifies that G_1 and G_2 are normal algebraic subgroups of $\mathbb{U}_3$. Moreover, their successive quotients

$$G_0/G_1 \xrightarrow{a_{12}} \mathbb{G}_a, \quad G_1/G_2 \xrightarrow{a_{23}} \mathbb{G}_a, \quad G_2/G_3 = G_2.$$

are all isomorphic to $\mathbb{G}_a$ as k-groups, where we denote as a_{ij} the map assigning to a matrix its coordinate (i,j). Finally, the series is easily seen to be central, so it is nilpotent. □

Proposition 1.2.5. *Every unipotent algebraic group over k admits a central normal series whose successive quotients are isomorphic to algebraic subgroups of the additive group $\mathbb{G}_a$. In particular, every unipotent algebraic group is* ***nilpotent****.*

Proof. First, we prove the following lemma on subnormal series : consider $G = G_0 \supset G_1 \supset \cdots \supset G_s = 1$ a subnormal series and let H be an algebraic subgroup of G. Then by setting $H_i := H \cap G_i$ for all $i = 0, \dots, s$ we obtain a subnormal series for H, such that each H_i/H_{i+1} is isomorphic to a subgroup of G_i/G_{i+1}. By Theorem 1.1.11 every unipotent group H can be realized as a subgroup of $G = \mathbb{U}_n$, so we conclude by applying Lemma 1.2.4.
By definition of subnormal series, each G_i is normal in G_{i+1}. Moreover, $H_i \cap H_{i+1} = H_{i+1}$, so by the isomorphism theorem (see [Mil17, Theorem 5.52]),

$$H_i/H_{i+1} = H_i/H_i \cap G_{i+1} \simeq H_i \cdot G_{i+1}/G_{i+1},$$

and the last term is an algebraic subgroup of G_i/G_{i+1}. □

Corollary 1.2.6. *Let G be a smooth connected unipotent algebraic group over k. If k is algebraically closed, then G admits a composition series whose successive quotients are isomorphic to $\mathbb{G}_a$.*

Proof. By Proposition 1.2.5, there exists a central normal series $(N_i)_{i=0}^s$, with successive quotients isomorphic to algebraic subgroups of $\mathbb{G}_a$. If we remplace each N_i by its identity component N_i^o, this gives a chain of connected normal subgroups of G having successive quotients of dimension less than or equal to 1. If we eliminate all repetitions, all successive quotients will be one-dimensional subgroups of $\mathbb{G}_a$, hence isomorphic to the additive group. □

1.2.3 Homomorphisms to $\mathbb{G}_a$

There is a useful characterisation of unipotent algebraic groups in terms of k-homomorphisms to the additive group. This provides an alternative definition of unipotency, which does not need linear representations : for example, it is the one given in [DG, IV, §2, 2.1].

Proposition 1.2.7. *Let G be an algebraic group over k, then it is unipotent if and only if every nontrivial k-subgroup of it admits a nontrivial homomorphism to $\mathbb{G}_a$.*

Proof. Let G be unipotent, and consider a k-subgroup H of G. By 1.1.12, H is unipotent too, so by 1.2.5 it admits a nontrivial algebraic subgroup of $\mathbb{G}_a$ as a quotient. The quotient map gives a nontrivial homomorphism $H \to \mathbb{G}_a$.
Now, let us assume that all k-subgroups of G admit nontrivial homomorphism to the additive group. In particular there exists a nontrivial k-homomorphism $\psi_1 \colon G \to \mathbb{G}_a$. Let us set $G_1 := \ker \psi_1$: it is either trivial or it admits a nontrivial $\psi_2 \colon G_1 \to \mathbb{G}_a$. By repeating this process, we obtain a descending series of algebraic subgroups $G \supset G_1 \supset \cdots \supset G_n \supset \cdots$ such that each G_{i+1} is normal in G_i. Moreover, algebraic subgroups satisfy the descending chain condition, hence this series must terminate in 1 and it gives a subnormal series for G. Its successive quotients are isomorphic to algebraic subgroups of $\mathbb{G}_a$, so G is actually obtained by successive extensions of such subgroups, which are unipotent. By Corollary 1.1.12, we conclude that G is unipotent. □

Commutative unipotent groups over perfect fields

The aim of this part is to give an overview of the structure of commutative unipotent groups over a perfect field, following [DG]. First, the Frobenius and Verschiebung morphisms are introduced, followed by the groups of Witt vectors and some results on their extensions. These elements allow to define Dieudonné modules over a field and to establish an equivalence of categories between them and unipotent commutative groups.

2.1 Frobenius and Verschiebung

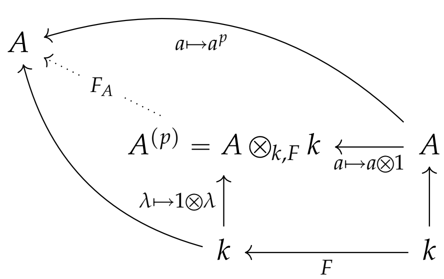
This first subsection applies to any ground field k of characteristic $p > 0$, not necessarily perfect. Our aim is to introduce for an affine algebraic k-group G a twisted version of the Frobenius endomorphism of k, defining it in such a way that it is a k-group homomorphism.
Let X be any k-scheme of finite type. We will restrict to the affine case, which is enough for our purposes, in order to simplify notations. The **absolute Frobenius morphism** of X is the scheme morphism which acts as the identity on the topological space $|X|$ and as $h \mapsto h^p$ on the sections of $\mathcal{O}_X$ over any open subset of X. However, this does not define a k-scheme morphism, since the frobenius $F\colon k \to k$ does not coincide with the identity in general. Therefore, we are led to introducing the following definitions.

Definition 2.1.1. Let A be a k-algebra. We define $A^{(p)}$ as the tensor product $A \otimes_{k,F} k$.

Definition 2.1.2. The (relative) **Frobenius morphism** of a k-algebra A is the k-algebra homomorphism

$$F_A\colon A^{(p)} \longrightarrow A$$

obtained via the following diagram by the universal property of the tensor product:



In other words, it is given by $F_A(a \otimes \lambda) = \lambda a^p$, so it is the one that makes the Frobenius into a k-algebra morphism.

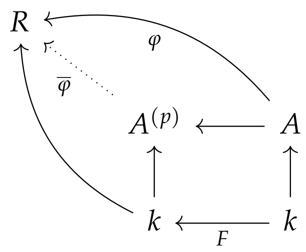
Now let us consider $X = \operatorname{Spec} A$ and denote $X^{(p)} = \operatorname{Spec} A^{(p)}$ its base change with respect to the Frobenius morphism. We denote the k-scheme morphism associated to F_A as

$$F_X \colon X \longrightarrow X^{(p)}.$$

It is called the relative Frobenius morphism of X.
Now, let us restrict to the case of an algebraic group over k.

Proposition 2.1.3. *Let $G = \operatorname{Spec} A$ be an algebraic group over k. Then $G^{(p)}$ is an algebraic group and the morphism $F_G \colon G \to G^{(p)}$ is a k-homomorphism.*

Proof. It suffices to prove that the functor of points of $G^{(p)}$ is group-valued. Let us consider a k-algebra R and denote ${}_F R$ the k-algebra given by $k \xrightarrow{F} k \to R$. By the following diagram,



there is a bijection

$$\operatorname{Hom}_{(\mathrm{k-\mathbf{Alg}})}(A, {}_F R) \longrightarrow \operatorname{Hom}_{(\mathrm{k-\mathbf{Alg}})}(A^{(p)}, R), \quad \varphi \longmapsto \overline{\varphi}$$

hence the functor of points of $G^{(p)}$ is $G^{(p)}(R) = \operatorname{Hom}_{(k-\mathbf{Sch})}(\operatorname{Spec} R, G^{(p)}) = \operatorname{Hom}_{(\mathrm{k-\mathbf{Alg}})}(A^{(p)}, R) = \operatorname{Hom}_{(\mathrm{k-\mathbf{Alg}})}(A, {}_F R) = G({}_F R)$ so it takes values in the category $(\mathbf{Grp})$. □

Remark 2.1.4. Since it is defined by the universal property of the fiber product, the Frobenius morphism is functorial : for all k-scheme morphisms $\varphi \colon X \to Y$, the following diagram commutes

$$\begin{array}{ccc} X & \xrightarrow{F_X} & X^{(p)} \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi^{(p)}} \\ Y & \xrightarrow{F_Y} & Y^{(p)}. \end{array}$$

We will now introduce with a bit more work a dual notion to the Frobenius, called the Verschiebung morphism: the word means "shift" in English, while it is often called "décalage" by French authors. This section mainly follows [DG, IV, §3, 4].

Let B be a k-algebra and $X := \operatorname{Spec} B$. The symmetric group $\mathcal{S}_p$ acts on the p-th tensor product $\bigotimes^p B := B \otimes \cdots \otimes B$ by

$$\sigma(v_1 \otimes \cdots \otimes v_p) = v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(p)}, \quad \text{for all } \sigma \in \mathcal{S}_p$$

defining an action of $\mathcal{S}_p$ on the k-scheme $X^p := \operatorname{Spec}(\bigotimes^p B)$, which is not to be confused with the Frobenius twist $X^{(p)}$ that we introduced above. Let $\mathrm{TS}^p(B)$ be the k-algebra of symmetric tensors of order p over B and set

$$S^p X := \operatorname{Spec}(\mathrm{TS}^p(B)).$$

Remark 2.1.5. Since $\mathrm{TS}^p(B)$ is by definition the greatest k-subalgebra of $\bigotimes^p B$ on which $\mathcal{S}_p$ acts trivially, it is the ring of invariants under the action of $\mathcal{S}_p$. Thus, the corresponding canonical morphism

$$q_X \colon X^p \longrightarrow S^p X$$

realizes $S^p X$ as the quotient of X^p by the symmetric group $\mathcal{S}_p$. By the universal property of the quotient, for all affine k-schemes Y and all $\mathcal{S}_p$-invariant k-scheme morphism $\psi \colon X^p \to Y$ there exists a unique $\overline{\psi} \colon S^p X \to Y$ such that the following diagram commutes.

$$\begin{array}{ccc} X^p & \xrightarrow{\quad\psi\quad} & Y \\ & {\scriptstyle q_X}\searrow & \nearrow{\scriptstyle \exists!\,\overline{\psi}} \\ & S^p X & \end{array}$$

The following lemma allows us to see $X^{(p)}$ as a closed subscheme of $S^p X$.

Lemma 2.1.6. *Let B be a k-algebra and denote $\mathbf{s}$ the symmetrizing operator*

$$\mathbf{s} \colon \bigotimes^p B \longrightarrow \mathrm{TS}^p(B), \quad v_1 \otimes \cdots \otimes v_p \longmapsto \sum_{\sigma \in \mathcal{S}_p} v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(p)}.$$

The canonical map

$$B^{(p)} = B \otimes_{k,F} k \longrightarrow \mathrm{TS}^p(B), \quad v \otimes \lambda \longmapsto \lambda(v \otimes \cdots \otimes v)$$

induces an isomorphism of k-algebras

$$B^{(p)} \simeq \mathrm{TS}^p(B)/\mathbf{s}(\bigotimes^p B).$$

We will denote as v^p the image of $v \otimes \cdots \otimes v$ in the quotient, so the isomorphism is given by $v \otimes \lambda \mapsto \lambda v^p$.

Proof. Let $(e_i)_{i \in I}$ be a basis of B as a k-vector space. For any $J = (j_1, \ldots, j_p) \in I^p$, denote as $e_J := e_{j_1} \otimes \cdots \otimes e_{j_p}$ and call $\omega(J) \subset I^p$ the orbit of J under the action of $\mathcal{S}_p$ given by $(\sigma, J) \mapsto (j_{\sigma(1)}, \ldots, j_{\sigma(p)})$. If $\omega = \omega(J)$ is such an orbit, set $e_\omega := \sum_{J' \in \omega} e_{J'}$. The collection $(e_\omega)_\omega$ give a k-basis of $TS^p(B)$ and

$$\mathbf{s}(e_J) = \mathbf{s}(e_{j_1} \otimes \cdots \otimes e_{j_p}) = N \cdot e_{\omega(J)} \qquad \text{for some } N \in \mathbb{N}.$$

In particular, N is the cardinality of the stabilizer of J in $\mathcal{S}_p$. Hence, $TS^p(B)$ is the direct sum of $\mathbf{s}(\bigotimes^p B)$ and of the k-vector subspace having as basis $\{e_J \colon j_1 = \ldots = j_p\}$. □

Having identified $B^{(p)}$ with a quotient of $\mathrm{TS}^p(B)$, the corresponding k-scheme morphism

$$i_X \colon X^{(p)} \longrightarrow S^p X$$

is a closed immersion.

Lemma 2.1.7. *Let B be a k-algebra and $X = \operatorname{Spec} B$. The following diagram*

$$\begin{tikzcd} X^p \arrow[d, "q_X"] & X \arrow[l, "\delta"'] \arrow[d, "F_X"] \\ S^pX & X^{(p)} \arrow[l, "i_X"] \end{tikzcd}$$

commutes, where $\delta\colon X \to X^p$ denotes the diagonal morphism.

Proof. Indeed, it corresponds to the diagram of k-algebras

$$\begin{tikzcd} \bigotimes^p B \arrow[r, "\mu"] & B \arrow[d, "F_B"] \\ \mathrm{TS}^p(B) \arrow[u] \arrow[r] & B^{(p)} \end{tikzcd}$$

with $\mu(v_1 \otimes \cdots \otimes v_p) = v_1 \cdot \ldots \cdot v_p$, $F_B(v \otimes \lambda) = \lambda v^p$ and the quotient map on the bottom is given by Lemma 2.1.6. Hence, it is commutative by definition of $\mathbf{s}$. □

Now, let $G = \operatorname{Spec} A$ be a **commutative** algebraic group over k. Denote as $\pi_p\colon G^p \to G$ the multiplication by p, i.e. the morphism given by

$$\pi_p\colon G(R) \times \cdots \times G(R) \longrightarrow G(R), \quad (g_1, \ldots, g_p) \longmapsto g_1 + \ldots + g_p,$$

for all k-algebras R, where the group law on G is written additively. It corresponds to the k-algebra morphism $\Delta^p = \Delta \otimes \cdots \otimes \Delta\colon A \to A^p$.
For a k-scheme morphism $f\colon X \to G$, corresponding to a k-algebra morphism $f^*\colon A \to B$, let $f^p\colon X^p \to G^p$ be the morphism given by

$$\bigotimes^p A \longrightarrow \bigotimes^p B, \quad a_1 \otimes \cdots \otimes a_p \longmapsto f^*(a_1) \otimes \cdots \otimes f^*(a_p).$$

By commutativity of G, the map $\pi_p \circ f^p$ is $\mathcal{S}_p$-invariant, so by Remark 2.1.5 there exists a unique $\overline{f^p}\colon S^pX \to G$ factorising it.

Definition 2.1.8. With the above notations, the morphism

$$f^V := \overline{f^p} \circ i_X\colon X^{(p)} \longrightarrow G$$

is called **induced by Verschiebung** by f. In other words, f^V is defined by the following commutative diagram

$$\begin{tikzcd} X^p \arrow[r, "q_X"] \arrow[d, "f^p"'] \arrow[dr, "f_p"] & S^pX \arrow[d, "\overline{f^p}"] & X^{(p)} \arrow[l, "i_X"'] \arrow[dl, dotted, "f^V"] \\ G^p \arrow[r, "\pi_p"] & G & \end{tikzcd}$$

Lemma 2.1.9. *Let $f\colon X \to G$ as above.*

(a) For all affine k-schemes Y and all k-scheme morphisms $g\colon Y \to X$,

$$(f \circ g)^V = f^V \circ g^{(p)}.$$

(b) We have

$$f^V \circ F_X = p \cdot f \colon X \longrightarrow G,$$

where for all k-algebras R, $p \cdot f \colon X(R) \longrightarrow G(R), \quad x \longmapsto p \cdot f(x) = f(x) + \ldots + f(x).$

Proof. (a) : The following diagram is commutative

$$\begin{array}{ccccc} Y^p & \xrightarrow{q_X} & S^pY & \xleftarrow[i_Y]{} & Y^{(p)} \\ \downarrow{\scriptstyle g^p} & & \downarrow{\scriptstyle S^pg} & & \downarrow{\scriptstyle g^{(p)}} \\ X^p & \xrightarrow{q_X} & S^pX & \xleftarrow[i_X]{} & X^{(p)} \end{array}$$

so together with the diagram in Definition 2.1.8, by uniqueness of the construction we obtain $(f \circ g)^V = f^V \circ g^{(p)}$.
(b) : As seen in Lemma 2.1.7, $i_X \circ F_X = q_X \circ \delta$. Hence, $f^V \circ F_X = \overline{f^p} \circ i_X \circ F_X = \overline{f^p} \circ q_X \circ \delta$, which by the diagram in Definition 2.1.8 is equal to $f_p \circ \delta = p \cdot f$. □

Definition 2.1.10. Let G be a commutative algebraic group over k. Using the above notations, the morphism $(\mathrm{id}_G)^V$ is called the **Verschiebung morphism** of G and is denoted V_G.

In particular, V_G is equal to $\overline{(\mathrm{id}_G)^p} \circ i_G$. Notice that, by applying Lemma 2.1.9 to $f = \mathrm{id}_G$, we get $h^V = V_G \circ h^{(p)}$ for all k-scheme morphisms $h\colon X \to G$.

Example 2.1.11. Let $G = \mathbb{G}_a = \operatorname{Spec} k[T]$. The morphism $\pi_p\colon \mathbb{G}_a^p \to \mathbb{G}_a$ corresponds to

$$\begin{aligned}\Delta^p\colon k[T] \longrightarrow \bigotimes^p k[T], \quad T \longmapsto & 1 \otimes \cdots \otimes 1 \otimes T + 1 \otimes \cdots \otimes T \otimes 1 + \ldots + T \otimes 1 \otimes \ldots \otimes 1 \\ &= \frac{1}{(p-1)!}\mathbf{s}(1 \otimes \cdots \otimes 1 \otimes T) \in \mathbf{s}\left(\bigotimes^p k[T]\right),\end{aligned}$$

hence in particular $\overline{(\mathrm{id}_G)^p}$ is zero, so $V_{\mathbb{G}_a} = \overline{(\mathrm{id}_G)^p} \circ i_{\mathbb{G}_a} = 0$.

Let us state a few fundamental properties, which justify the fact that the Verschiebung is seen as a dual of the Frobenius. Finally, we conclude this subsection with a lemma showing that the Verschiebung morphism behaves very differently for unipotent groups compared to the case of groups of multiplicative type.

Proposition 2.1.12. *Let G and H be commutative algebraic groups over k.*

(i) The Verschiebung morphism $V_G\colon G^{(p)} \to G$ *is a k-homomorphism.*

(ii) (functoriality) Let $\varphi\colon G \to H$ *be a k-homomorphism, then*

$$\varphi \circ V_G = V_H \circ \varphi^{(p)}.$$

(iii) The formation of the Verschiebung commutes with extensions of the base field : for any extension k'/k, we have $V_{G_{k'}} = V_G \otimes_k k'$.

(iv) (duality) The following equalities hold :

$$V_G \circ F_G = p \cdot \mathrm{id}_G, \quad \text{and} \quad F_G \circ V_G = p \cdot \mathrm{id}_{G^{(p)}} .$$

Proof. (i) : See [DG, II, §1, 1.5].
(ii) : By Lemma 2.1.9 (a), $\varphi^V = (\mathrm{id}_H \circ \varphi)^V = (\mathrm{id}_H)^V \circ \varphi^{(p)} = V_H \circ \varphi^{(p)}$. On the other hand, $\varphi \circ V_G$ verifies the suitable diagram in Definition 2.1.8, so by uniqueness it must coincide with φ^V.
(iii) : All morphisms involved in the definition of V_G commute with extensions of the base field. Actually, the construction works on any base ring and automatically commutes with any base change, see [DG, IV,§3, 4.6].
(iv) : By Lemma 2.1.9 (b) applied to $f = \mathrm{id}_G$, we have $V_G \circ F_G = (\mathrm{id}_G)^V \circ F_G = p \cdot \mathrm{id}_G$. Now, the Frobenius morphism is functorial as seen in Lemma 2.1.4 : by applying it to $\varphi = V_G$, we get $F_G \circ V_G = (V_G)^{(p)} \circ F_{G^{(p)}}$. Moreover, by (iii), taking as base change the Frobenius endomorphism $F \colon k \to k$, the map $(V_G)^{(p)}$ equals $V_{G^{(p)}}$, hence by (ii) we obtain

$$F_G \circ V_G = V_{G^{(p)}} \circ F_{G^{(p)}} = p \cdot \mathrm{id}_{G^{(p)}}$$

and conclude. □

Lemma 2.1.13. *Let G be a commutative algebraic group over k. The following are equivalent:*

(1) The Verschiebung V_G is an isomorphism,

(2) The Verschiebung V_G is an epimorphism,

(3) The group G is of multiplicative type.

Moreover, the group G is unipotent if and only if for every quotient H of G there exists an integer n such that $V_H^n = 0$.

Proof. $(1) \Rightarrow (2)$: trivial.
$(2) \Rightarrow (3)$: Let $f \colon G \to \mathbb{G}_a$ be a k-homomorphism, then by Proposition 2.1.12 and Example 2.1.11, $f \circ V_G = V_{\mathbb{G}_a} \circ f^{(p)} = 0$, hence f is trivial. By [Mil17, 12.18], this shows that G is of multiplicative type.
$(3) \Rightarrow (1)$: By Proposition 2.1.12, we can extend scalars and assume that the group G is diagonalizable, i.e. of the form $\mathrm{Spec}(k[M])$ for a suitable abelian group of finite type M. In this case, M identifies with the group of characters of G and the morphism π_p corresponds to the k-algebra homomorphism

$$\Delta^p \colon k[M] \longrightarrow \bigotimes^p k[M], \quad m \longmapsto m \otimes \cdots \otimes m.$$

In particular, this implies that the Verschiebung morphism is an isomorphism (see [DG, IV, §3, 4.11]). Now, let us suppose that G is unipotent: since every algebraic quotient is unipotent too, it suffices to prove the claim for $H = G$. Let us consider $(G_i)_{i=0}^s$ a composition series of G having successive quotients isomorphic to algebraic subgroups of $\mathbb{G}_a$ and proceed by induction on s. If $s = 1$, we conclude that $V_G = 0$ by Example 2.1.11. If $s > 1$, by induction there exist integers n, m such that

$V^n_{G_1} = 0$ and $V^m_{G/G_1} = 0$. This last assertion means in particular that $V^m_G(G^{(p^m)}) \subset G_1$. Moreover, for all i the diagram

$$\begin{array}{ccccc} G_1^{(p^i)} & \longrightarrow & G^{(p^i)} & \longrightarrow & (G/G_1)^{(p^i)} \simeq G^{(p^i)}/G_1^{(p^i)} \\ \downarrow V^i_{G_1} & & \downarrow V^i_G & & \downarrow V^i_{G/G_1} \\ G_1 & \longrightarrow & G & \longrightarrow & G/G_1 \end{array}$$

commutes. Hence, we can factorise V^{n+m}_G as

$$G^{(p^{n+m})} \xrightarrow{(V^m_G)^{(p^n)}} G_1^{(p^n)} \xrightarrow{V^n_{G_1}} G_1 \subset G$$

so we obtain $V^{n+m}_G = 0$. □

2.2 Witt groups

Throughout the rest of this chapter, k will denote a perfect field of characteristic $p > 0$. We will now define the group of Witt vectors, which play a fundamental role in classifying commutative unipotent groups over k. The main reference other than [DG] is [Rab14].

2.2.1 Definition

Definition 2.2.1. Let $n \in \mathbb{N}$. The **n-th Witt polynomial** is the element of $\mathbb{Z}[X_0, X_1, X_2 \ldots] = \mathbb{Z}[\underline{X}]$ given by

$$w_n(\underline{X}) := X_0^{p^n} + pX_1^{p^{n-1}} + p^2X_2^{p^{n-2}} + \ldots + p^nX_n.$$

Let us denote as $\mathbb{A}^{\mathbb{N}}_{\mathbb{Z}}$ the scheme $\operatorname{Spec}\mathbb{Z}[\underline{X}]$. Then each w_n defines a scheme morphism, still denoted as $w_n \colon \mathbb{A}^{\mathbb{N}}_{\mathbb{Z}} \to \mathbb{A}^1_{\mathbb{Z}}$, given on the functor of points by the set-theoretic maps

$$R^{\mathbb{N}} \longrightarrow R, \quad \underline{x} \longmapsto (w_n(\underline{x})),$$

for all rings R. Let us call Φ the scheme morphism having w_n as its n-th component, i.e.

$$\Phi \colon \mathbb{A}^{\mathbb{N}}_{\mathbb{Z}} \longrightarrow \mathbb{A}^{\mathbb{N}}_{\mathbb{Z}}, \quad \underline{x} \longmapsto (w_n(\underline{x}))_{n\in\mathbb{N}}.$$

Remark 2.2.2. Notice that we can express all variables X_n as polynomials

$$X_n \in \mathbb{Z}[p^{-1}][w_0, w_1, \ldots w_{n-1}] \subset \mathbb{Z}[p^{-1}, w_0, w_1, \ldots, w_i, \ldots].$$

For instance, $X_0(\underline{w}) = w_0$. If we suppose the statement to be true for all X_j with $j \leqslant n$, then the equality

$$w_{n+1} = X_0(\underline{w})^{p^{n+1}} + pX_1(\underline{w})^{p^n} + \ldots + pX_n(\underline{w})^p + p^{n+1}X_{n+1}$$

allows us to express X_{n+1} in the desired form. For example,

$$X_1 = \frac{1}{p}\left(w_1 - X_0^p\right) = \frac{1}{p}\left(w_1 - w_0^p\right), \tag{2.1}$$

$$X_2 = \frac{1}{p^2}\left(w_2 - \frac{1}{p^{p-1}}w_1^p - \frac{1}{p^{p-1}}w_0^{2p} - w_0^{p^2}\right). \tag{2.2}$$

In other words, the map

$$\Phi_{\mathbb{Z}[p^{-1}]}\colon \mathbb{A}^N \otimes_{\mathbb{Z}} \mathbb{Z}[p^{-1}] \longrightarrow \mathbb{A}^N \otimes_{\mathbb{Z}} \mathbb{Z}[p^{-1}]$$

is a scheme isomorphism.

Now, let us denote as $\mathscr{O}$ the scheme $\mathbb{A}^1_{\mathbb{Z}}$, together with its canonical ring scheme structure. The aim is to use Φ to define a new ring structure on $\mathbb{A}^{\mathbb{N}}_{\mathbb{Z}}$.

Definition 2.2.3. The **ring of Witt vectors** is the ring scheme having as underlying scheme $\mathbb{A}^{\mathbb{N}}_{\mathbb{Z}}$, equipped with the addition and multiplication laws given on the functor of points by

$$\underline{x} \boxplus \underline{y} := \Phi^{-1}(\Phi(\underline{x}) + \Phi(\underline{y})), \tag{2.3}$$

$$\underline{x} \boxdot \underline{y} := \Phi^{-1}(\Phi(\underline{x}) + \Phi(\underline{y})), \tag{2.4}$$

for all $\underline{x}, \underline{y} \in R^{\mathbb{N}}$, for all rings R, where the operations on the right hand side are done componentwise, i.e. using the ring structure of $\mathscr{O}^{\mathbb{N}}$. For any element $\underline{x} \in R^{\mathbb{N}}$, the coordinates x_i are called its **Witt components** and the coordinates $w_n(\underline{x})$ its **ghost components**.

Proof. By Remark 2.2.2, these operations are well defined after a base change to $\mathbb{Z}[p^{-1}]$: it suffices to transport the ring structure by means of the $\mathbb{Z}[p^{-1}]$-isomorphism $\Phi_{\mathbb{Z}[p^{-1}]}$. Hence, for all $i \in \mathbb{N}$, there exist unique polynomials S_i, $P_i \in \mathbb{Z}[X_0, \dots X_i, Y_0, \dots, Y_i] \subset \mathbb{Z}[\underline{X}, \underline{Y}]$ such that

$$w_n(S_0(\underline{X}, \underline{Y}), S_1(\underline{X}, \underline{Y}), \dots) = w_n(\underline{X}) + w_n(\underline{Y}),$$
$$w_n(P_0(\underline{X}, \underline{Y}), P_1(\underline{X}, \underline{Y}), \dots) = w_n(\underline{X}) \cdot w_n(\underline{Y}).$$

It remains to show that those polynomials actually have integer coefficients, so the ring structure is defined over $\mathbb{Z}$. Let us discuss in detail the case $i = 0$ and $i = 1$, for the general case see [DG, V, §1, 1.1]. For instance,

$$\Phi^{-1}((x_0, x_0^p, \dots) + (y_0, y_0^p, \dots)) = (x_0 + y_0, \dots) \quad \text{and} \quad \Phi^{-1}((x_0, x_0^p, \dots) \cdot (y_0, y_0^p, \dots)) = (x_0 y_0, \dots),$$

hence $S_0(\underline{X}, \underline{Y}) = X_0 + Y_0$ and $P_0(\underline{X}, \underline{Y}) = X_0 Y_0$. Moreover, by 2.1

$$(x_0, x_1, 0, \dots) \boxplus (y_0, y_1, 0, \dots) = \Phi^{-1}((x_0, x_0^p + p x_1, \dots) + (y_0, y_0^p + p y_1, \dots)) =$$
$$(x_0 + y_0, \frac{1}{p}(x_0^p + y_0^p + p x_1 + p y_1 - (x_0 + y_0)^p), \dots) = (x_0 + y_0, x_1 + y_1 - \frac{1}{p} \sum_{i=1}^{p-1} \binom{p}{i} x_0^i y_0^{p-1}, \dots),$$

so we get

$$S_1(\underline{X}, \underline{Y}) = X_1 + Y_1 - \frac{1}{p} \sum_{i=1}^{p-1} \binom{p}{i} X_0^i Y_0^{p-i}.$$

Analogously, we find that

$$P_1(\underline{X}, \underline{Y}) = P_1(X_0, X_1, Y_0, Y_1) = X_1 Y_0^p + X_0^p Y_1 + p X_1 Y_1.$$

□

Definition 2.2.4. Let A be a ring. The **A-group of Witt vectors**, which we will still denote as W_A, is the underlying group scheme, having as commutative group law the one defined by the polynomials S_i above.

Definition 2.2.5. Let $n \in \mathbb{N}$. The ring scheme W_n is defined as having as underlying scheme $\mathbb{A}^n_{\mathbb{Z}}$, while addition and multiplication are obtained by truncating the ones in W :

$$(a_0, \dots, a_{n-1}) \boxplus (b_0, \dots, b_{n-1}) = (S_0(a_0, b_0), \dots, S_{n-1}(a_0, \dots, a_{n-1}, b_0, \dots, b_{n-1})),$$
$$(a_0, \dots, a_{n-1}) \boxdot (b_0, \dots, b_{n-1}) = (P_0(a_0, b_0), \dots, P_{n-1}(a_0, \dots, a_{n-1}, b_0, \dots, b_{n-1})).$$

This is called the **scheme of Witt vectors of lenght n** and for a ring A an element in $W_n(A)$ is called a Witt vector of length n with coefficients in A.

In particular, notice that $W_1 \simeq \mathscr{O}$, hence as group scheme it is isomorphic to the additive group $\mathbb{G}_a$.

Let us introduce two collections of morphisms between Witt groups: the first shows that the group W has a natural projective limit structure, while the second will correspond to the Verschiebung morphism in this particular case.

For all $n \in \mathbb{N}$, let us denote as π_n the canonical projection

$$\pi_n \colon W_{n+1} \longrightarrow W_n$$
$$(a_0, \dots, a_n) \mapsto (a_0, \dots, a_{n-1}),$$

which are in particular morphisms of ring valued functors. Moreover, they induce projections $\pi_{n,m} \colon W_{n+m} \to W_m$ for all $n, m \in \mathbb{N}$, hence a projective limit structure

$$W = \varprojlim_{n \in \mathbb{N}} W_n.$$

Now, let us consider the collection of the shifting maps

$$\mathcal{I}_n \colon W_n \longrightarrow W_{n+1}$$
$$(a_0, \dots, a_{n-1}) \mapsto (0, a_0, \dots, a_{n-1}).$$

Since these maps are compatible with the projections, they induce by passing to the projective limit a morphism

$$\mathcal{I} \colon \varprojlim_{n \in \mathbb{N}} W_n = W \longrightarrow \varprojlim_{n \in \mathbb{N}} W_{n+1} = W' \simeq W$$
$$(a_0, a_1, \dots) \mapsto (0, a_0, a_1, \dots).$$

Let us denote as $\mathcal{I}_{n,m} \colon W_n \to W_{n+m}$ the shifting morphism obtained by iterating $\mathcal{I}$ and truncating, i.e. $\mathcal{I}_{n,m}(a_0, \dots, a_{n-1}) = (0, \dots, 0, a_0, \dots, a_{n-1})$. The following sequence of group-valued functors is exact:

$$0 \longrightarrow W_n \xrightarrow{\mathcal{I}_{n,m}} W_{n+m} \xrightarrow{\pi_{n,m}} W_m \longrightarrow 0.$$

Lemma 2.2.6. *Let us consider the ring $W(k)$. For all elements $w = (a_0, a_1, a_2, \dots)$, the following equality* *holds*

$$p \boxdot w = (0, 1, 0 \ldots) \boxdot (a_0, a_1, a_2, \ldots) = (0, a_0^p, a_1^p, a_2^p, \ldots).$$

Proof. We have explicit expressions for P_0 and P_1 above in Definition 2.2.3: this gives $P_0(p, w) = 0 \cdot a_0 = 0$ and $P_1(p, w) = a_1 \cdot 0 + 1 \cdot a_1^p + p^2 a_1 = a_1^p$. For the general calculation, see [DG, V,§1, 1.7]. ☐

Remark 2.2.7. Let A be a ring of characteristic p. The following commutative diagram made up of cartesian squares

$$\begin{array}{ccccccc} W_A^{(p)} & \longrightarrow & W_A & \longrightarrow & W_{\mathbb{F}_p}) & \longrightarrow & W \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \operatorname{Spec}(A) & \xrightarrow{F_A} & \operatorname{Spec}(A) & \longrightarrow & \operatorname{Spec}(\mathbb{F}_p) & \longrightarrow & \operatorname{Spec} \mathbb{Z} \end{array}$$

shows that $W_A^{(p)} = W_A$ and analogously we have $W_{n,A}^{(p)} = W_{n,A}$ for all n.

Lemma 2.2.8. *Let A be k-algebra. The Verschiebung morphism $V_{W_A} \colon W_A \to W_A$ is equal to $\mathcal{I}_{W_A}$.*

Proof. By functoriality, it suffices to prove it for $A = \mathbb{F}_p$. In this case, the Frobenius map $F_{W_{\mathbb{F}_p}}$ is a homomorphism of commutative $\mathbb{F}_p$-groups. Since both $V_{W_{\mathbb{F}_p}} \circ F_{W_{\mathbb{F}_p}}$ and $\mathcal{I}_{W_{\mathbb{F}_p}} \circ F_{W_{\mathbb{F}_p}}$ are equal to $p \cdot \mathrm{id}_{W_{\mathbb{F}_p}}$ by Remark 2.2.6, then

$$(V_{W_{\mathbb{F}_p}} - \mathcal{I}_{W_{\mathbb{F}_p}}) \circ F_{W_{\mathbb{F}_p}} = 0$$

and we are done because $F_{W_{\mathbb{F}_p}}$ is an epimorphism of algebraic groups over $\mathbb{F}_p$, because the corresponding $\mathbb{F}_p$-algebra homomorphism is injective. ☐

2.2.2 Extensions of Witt groups

Let us consider the following exact sequence:

$$0 \longrightarrow W_n \xrightarrow{\mathcal{I}_n} W_{n+1} \xrightarrow{\pi_{n,1}} \mathbb{G}_a \longrightarrow 0$$

and denote as $\mathcal{E}_n$ the element of $\operatorname{Ext}^1(\mathbb{G}_a, W_{n,k})$ corresponding to the isomorphism class of this extension.

Lemma 2.2.9. *Let us consider the morphisms $\mathcal{I}_n \colon W_{n,k} \to W_{n+1,k}$ and $\pi_{1,n} \colon W_{n+1,k} \to W_{n,k}$, which induce maps*

$$(\mathcal{I}_n)_* \colon \operatorname{Ext}^1(\mathbb{G}_a, W_{n,k}) \longrightarrow \operatorname{Ext}^1(\mathbb{G}_a, W_{n+1,k}),$$
$$(\pi_{1,n})_* \colon \operatorname{Ext}^1(\mathbb{G}_a, W_{n+1,k}) \longrightarrow \operatorname{Ext}^1(\mathbb{G}_a, W_{n,k}).$$

Then

$$(\mathcal{I}_n)_* \mathcal{E}_n = 0 \quad \textit{and} \quad (\pi_{1,n})_* \mathcal{E}_{n+1} = \mathcal{E}_n.$$

Proof. Let H be an extension obtained by pushforward of $W_{n+1,k}$ along the morphism $\mathcal{I}_n$: it is given by the following diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & W_{n,k} & \xrightarrow{\mathcal{I}_n} & W_{n+1,k} & \xrightarrow{\pi_{n,1}} & \mathbb{G}_a & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \mathcal{I}_n} & & \downarrow{\scriptstyle j} & & \| & & \\
1 & \longrightarrow & W_{n+1,k} & \underset{\sigma}{\overset{i}{\rightleftarrows}} & H & \longrightarrow & \mathbb{G}_a & \longrightarrow & 1
\end{array}$$

In particular, H is the quotient of $W_{n+1,k} \times W_{n+1,k}$ by the anti-diagonal action of $W_{n,k}$, i.e. we have the following equivalence relation: for all $x, y \in W_{n+1,k}$ and all $x \in W_{n,k}$,

$$(x, y) \sim (x + \mathcal{I}_n(z), y - \mathcal{I}_n(z)).$$

The morphisms i and j are then given by

$$i\colon x \longmapsto (x, 0), \quad j\colon y \longmapsto (0, -y)$$

and there is a canonical well-defined section of i,

$$\sigma\colon H \longrightarrow W_{n+1,k}, (x, y) \longmapsto x + y,$$

which splits the sequence, hence the extension is trivial.
The second statement follows from the definition of $\mathcal{E}_{n+1}$ and $\mathcal{E}_n$ as the isomorphism classes of $W_{n+2,k}$ and $W_{n+1,k}$ respectively and from the fact that the following diagram is cocartesian.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & W_{n+1,k} & \xrightarrow{\mathcal{I}_{n+1}} & W_{n+2,k} & \xrightarrow{\pi_{n+1,1}} & \mathbb{G}_a & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \pi_{1,n}} & & \downarrow{\scriptstyle \pi_{1,n+1}} & & \| & & \\
1 & \longrightarrow & W_{n,k} & \longrightarrow & W_{n+1,k} & \xrightarrow{\pi_{n,1}} & \mathbb{G}_a & \longrightarrow & 1.
\end{array}$$

□

Let us make a few remarks on endomorphisms of the additive group and apply them to our study of extensions of Witt groups.

Definition 2.2.10. The ring $k[\mathbf{F}]$ is the noncommutative ring of polynomials in the variable $\mathbf{F}$, with multiplication given by

$$\mathbf{F}\lambda = \lambda^p \mathbf{F}, \quad \text{for all } \lambda \in k.$$

Lemma 2.2.11. *The ring of endomorphisms of the additive k-group $\mathbb{G}_a$ is isomorphic to $k[\mathbf{F}]$.*

Proof. Let us denote as Δ the comultiplication map of $\mathcal{O}(\mathbb{G}_a) = k[T]$: an endomorphism of $\mathbb{G}_a$ corresponds to giving an element $P = \sum_l a_l T^l \in k[T]$ such that $\Delta P = P \otimes 1 + 1 \otimes P$. This means that for all l,

$$a_l(T^l \otimes 1 + 1 \otimes T^l) = a_l(T \otimes 1 + 1 \otimes T)^l$$

and this condition is satisfied if and only if P is of the form

$$b_0 T + b_1 T^p + \ldots + b_n T^{p^n}, \quad b_j \in k.$$

Now, let us denote as $\mathbf{F}$ the Frobenius endomorphism of $\mathbb{G}_a$: this gives an isomorphism

$$k[\mathbf{F}] \simeq \mathrm{End}(\mathbb{G}_a), \quad \sum_j b_j \mathbf{F}^j \longmapsto \sum_j b_j T^{p^j}.$$

□

Let G be a commutative algebraic group over k. Then $\mathrm{Ext}^1(G, \mathbb{G}_a)$ is a left $k[\mathbf{F}]$-module by considering the operation of pushforward along an endomorphism of $\mathbb{G}_a$; analogously $\mathrm{Ext}^1(\mathbb{G}_a, G)$ is a right $k[\mathbf{F}]$-module considering pullbacks.

Proposition 2.2.12. *Let H be a k-subgroup of $\mathbb{G}_a$ and $n \geqslant 1$. Then*

(a) The map $(\pi_{n-1,1})_* \colon \mathrm{Ext}^1(H, W_{n,k}) \to \mathrm{Ext}^1(H, \mathbb{G}_a)$ is bijective.

(b) Let $i \colon H \hookrightarrow \mathbb{G}_a$ be the inclusion morphism, then the induced map

$$i^* \colon \mathrm{Ext}^1(\mathbb{G}_a, W_{n,k}) \longrightarrow \mathrm{Ext}^1(H, W_{n,k})$$

is surjective.

(c) The left $k[\mathbf{F}]$-module $\mathrm{Ext}^1(\mathbb{G}_a, W_{n,k})$ is free with basis $\{\mathcal{E}_n\}$.

Proof. The proof is by induction on n, see [DG, V, §1, 2.2]. The proof shows that the assumption that the base field k is perfect is sufficient. □

Corollary 2.2.13. *Let*

$$0 \longrightarrow L \xrightarrow{j} M \xrightarrow{\varphi} \mathbb{G}_a$$

be an exact sequence of commutative k-groups and $f \colon L \to W_{n,k}$ a k-homomorphism. Then there exists a k-homomorphism $g \colon M \to W_{n+1,k}$ such that the following diagram is commutative

$$\begin{array}{ccc} L & \xrightarrow{\quad j \quad} & M \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} \\ W_{n,k} & \xrightarrow{\quad \mathcal{I}_n \quad} & W_{n+1,k}. \end{array}$$

Proof. Let H be the k-subgroup of $\mathbb{G}_a$ generated by the image of φ and see M as an extension of H by L. By functoriality of the pushforward of extensions, the following diagram commutes

$$\begin{array}{ccc} \mathrm{Hom}_{(\mathrm{k-}\mathbf{Grp})}(L, W_{n,k}) & \xrightarrow{\quad (-)_* \quad} & \mathrm{Ext}^1(H, W_{n,k}) \\ \downarrow{\scriptstyle \mathcal{I}_n \circ (-)} & & \downarrow{\scriptstyle (\mathcal{I}_n)_*} \\ \mathrm{Hom}_{(\mathrm{k-}\mathbf{Grp})}(L, W_{n+1,k}) & \xrightarrow{\quad (-)_* \quad} & \mathrm{Ext}(H, W_{n+1,k}). \end{array}$$

We claim that $(\mathcal{I}_n)_*$ is trivial: if this holds, then in particular the extension obtained by pushforward of M along $\mathcal{I}_n \circ f$ is trivial. Thus, there is a diagram of the following form, which gives the desired homomorphism g.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L & \xrightarrow{j} & M & \xrightarrow{\varphi} & H & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathcal{I}_n \circ f} & & \downarrow{\scriptstyle \varphi \times g} & & \| & & \\ 0 & \longrightarrow & W_{n+1,k} & \longrightarrow & H \times W_{n+1,k} & \longrightarrow & H & \longrightarrow & 0 \end{array}$$

It remains to show that $(\mathcal{I}_n)_* = 0$. By Proposition 2.2.12, i^* is surjective so it suffices to prove the claim for $H = \mathbb{G}_a$. Moreover, $\operatorname{Ext}^1(\mathbb{G}_a, W_{n,k})$ is free with basis $\{\mathcal{E}_n\}$, so we are done because $(\mathcal{I}_n)_* \mathcal{E}_n = 0$ as seen in Lemma 2.2.9. □

The following lemma will be a key results in the proofs of the next sections.

Lemma 2.2.14. *Let $m, n \geqslant 1$ and consider a commutative algebraic group G over k such that $V_G^n \colon G^{(p^n)} \to G$ is zero. For all k-homomorphisms $f \colon G \to W_{n+m,k}$, there exists a unique k-homomorphism $g \colon G \to W_{n,k}$ such that*

$$f = \mathcal{I}_{n,m} \circ g.$$

Proof. As seen in Lemma 2.2.8, $W_{n+m,k}^{(p)} = W_{n+m,k}$. By functoriality of the Verschiebung (see Proposition 2.1.12),

$$f \circ V_G^n = V_{W_{n+m,k}}^n \circ f^{(p^n)}$$

which is trivial because $V_G^n = 0$. Thus, we obtain a factorisation of $f^{(p^n)}$ by

$$G^{(p^n)} \xrightarrow{h} \ker V_{W_{n+m,k}}^n = \{(0, \ldots, 0, a_0, \ldots, a_{n-1})\} = \mathcal{I}_{n,m}(W_{n,k}).$$

Moreover, $\mathcal{I}_{n,m}$ is an isomorphism between W_n and $\ker V_{W_{n+m,k}}^n$ and $W_{n,k}$ is isomorphic to $W_{n,k}^{(p^n)}$, so h can be seen as a morphism $G^{(p^n)} \to W_{n,k}^{(p^n)}$.
Now, since the base field k is perfect, the functor $H \mapsto H^{(p)}$ from commutative algebraic k-groups into the same category is an equivalence. In particular, there exists a homomorphism $g \colon G \to W_{n,k}$ such that $h = g^{(p^n)}$. Thus, we obtain

$$f^{(p^n)} = (\mathcal{I}_{n,m})^{(p^n)} \circ h = (\mathcal{I}_{n,m})^{(p^n)} \circ g^{(p^n)} = (\mathcal{I}_{n,m} \circ g)^{(p^n)}$$

and we are done. □

The following result makes a first link between Witt vectors and general commutative unipotent groups, showing that such a group fits into a specific exact sequence involving Witt vectors.

Proposition 2.2.15. *Let U be a commutative unipotent algebraic group over k. There exists integers $n, r, s \in \mathbb{N}$ and an exact sequence of k-groups*

$$0 \longrightarrow G \longrightarrow W_{n,k}^r \longrightarrow W_{n,k}^s.$$

Proof. First, let us show the existence of a k-group monomorphism $\alpha \colon G \to W_{n,k}^n$. We will proceed by Noetherian induction: the statement is clearly true for $U = 1$ and we suppose it to be true for all proper algebraic subgroups of G. By Proposition 1.2.7, there exists a nontrivial k-homomorphism $f \colon G \to \mathbb{G}_a$. By applying the inductive hypothesis to $H := \ker f \subsetneq G$, there exists a monomorphism

$\gamma\colon H \to W^m_{m,k}$ for some m. By Corollary 2.2.13 applied to the components of f there exists a k-homomorphism $\alpha\colon G \to W^m_{m+1,k}$ such that the diagram

$$\begin{array}{ccc} H & \hookrightarrow & M \\ \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \alpha} \\ W_{m,k} & \xrightarrow{\mathcal{I}^m_m} & W^m_{m+1,k} \end{array}$$

commutes. This allows to take as monomorphism the map $G \to W^m_{m+1,k} \times W_{m+1,k}$ having as components α and $\mathcal{I}_{1,m} \circ f\colon G/H \to W_{m-1,k}$.
Now, let us consider such a monomorphism $\alpha\colon G \to W^r_{n,k}$ and denote as Q its cokernel. By the above consideration, there exists also a monomorphism $\alpha'\colon Q \to W^s_{m,k}$ for some integers m, s. By composing it with the quotient map $\pi\colon W^r_{n,k} \to Q$, one obtains an exact sequence of the form

$$0 \longrightarrow G \overset{\alpha}{\hookrightarrow} W^r_{n,k} \overset{\beta}{\longrightarrow} W^s_{m,k}.$$

If $m = n$ we are done, if $m < n$ it suffices to remplace β by $\mathcal{I}_{m,n-m} \circ \beta$, if $m > n$ we can apply Lemma 2.2.14 to get a k-homomorphism $\beta'\colon W^r_{n,k} \to W^s_{n,k}$ such that $\beta = \mathcal{I}^s_{n,m-n} \circ \beta'$ and remplacing β by β' still gives an exact sequence. □

2.3 Dieudonné modules

Let us fix some notations for the rest of this chapter : for $w = (a_0, a_1, \dots) \in W(k)$ and $n \in \mathbb{Z}$, we will denote as $w^{(p^n)}$ the element

$$w^{(p^n)} = F^n_{W(k)}(w) = (a_0^{p^n}, a_1^{p^n}, \dots).$$

The hypothesis of having a perfect base field allows us to take as n a negative integer.
Let us also recall that p identifies with $(0, 1, 0, \dots)$ in $W(k)$ and that $p \cdot w = \mathcal{I}(w^{(p)})$.

Definition 2.3.1. The **Dieudonné ring** over k is the ring $\mathbb{D}$ generated by $W(k)$ and two indeterminates $\mathbf{F}$ and $\mathbf{V}$ together with the relations

$$\mathbf{F}w = w^{(p)}\mathbf{F}, \quad w\mathbf{V} = \mathbf{V}w^{(p)}, \quad \mathbf{FV} = \mathbf{VF} = p.$$

By definition, $\mathbb{D}$ is a free $W(k)$-module, either for the right and for the left module structure, having as basis

$$\dots, \mathbf{F}^n, \dots, \mathbf{F}, 1, \mathbf{V}, \dots, \mathbf{V}^n, \dots$$

In other words, every element of $\mathbb{D}$ has a unique expression as a finite sum of the form

$$\sum_{n \geqslant 0} b_n \mathbf{F}^n + a + \sum_{n \geqslant 0} \mathbf{V}^n c_n, \quad a, b_n, c_n \in W(k).$$

Whenever needed we will denote it as $\mathbb{D}_k$ in order to specify the base field we are considering.

Definition 2.3.2. A **Dieudonné module** over k is a left $\mathbb{D}_k$-module.

Let us consider a perfect field extension K/k. The canonical map

$$W(K) \otimes_{W(k)} \mathbb{D}_k \longrightarrow \mathbb{D}_K$$

is given by

$$w \otimes \left(\sum_{n \geqslant 0} b_n \mathbf{F}^n + a + \sum_{n \geqslant 0} \mathbf{V}^n c_n \right) \longmapsto \sum_{n \geqslant 0} w b_n \mathbf{F}^n + wa + \sum_{n \geqslant 0} \mathbf{V}^n w^{(p^n)} c_n,$$

so it is an isomorphism because the Frobenius endomorphism of k is surjective.
Let M be a Dieudonné module over k. Then

$$W(K) \otimes_{W(k)} M = W(K) \otimes_{W(k)} \mathbb{D}_k \otimes_{\mathbb{D}_k} M \simeq D_K \otimes_{\mathbb{D}_k} M$$

so it has a natural structure of Dieudonné module over K, which is said to be the **extension of scalars** of M associated to K/k.

Let A be a k-algebra. For an element $w \in W(k)$, we will denote as w_A the corresponding element in $W(A)$ obtained via the morphism $k \to A$. Moreover, for $u \in W_n(A)$, we will denote as $w \cdot u$ the element obtained by truncating w_A and taking the product $\pi_n(w_A)u$ in $W_n(A)$.

Lemma 2.3.3. *Let A be a k-algebra and $n \geqslant 1$.*

(1) The group $M := W_n(A)$ together with the Frobenius and Verschiebung morphisms $\mathbf{F} = F_{W_n(A)}$ and $\mathbf{V} = V_{W_n(A)}$, equipped with the operation

$$w \cdot u = w_M \cdot u := (w^{(p^{1-n})})_A \cdot u, \quad \text{for all } u \in W_n(A), w \in W(k) \tag{2.5}$$

is a Dieudonné module over k.

(2) The map $\mathcal{I}_n \colon W_n(A) \to W_{n-1}(A)$ is a morphism of Dieudonné modules.

Proof. See [DG, V, §1, 3.2] □

The operation defined just above gives for all k-algebras A a morphism

$$\mathbb{D}_k \longrightarrow \mathrm{End}_A(W_n(A)) = \underline{\mathrm{End}}(W_{n,k})(A)$$

and it is by definition natural in A, hence induces a morphism of group-valued functors

$$\mathbb{D}_k \longrightarrow \underline{\mathrm{End}}(W_{n,k}) = \underline{\mathrm{Hom}}_{(\mathbf{k-Grp})}(W_{n,k}, W_{n,k}).$$

Moreover, the morphism $V^n_{W_{n,k}}$ is zero, so this actually defines a morphism

$$\rho_n \colon \mathbb{D}/\mathbb{D}\mathbf{V}^n \longrightarrow \mathrm{End}(W_{n,k})$$

Lemma 2.3.4. *For all $n \geqslant 1$, the homomorphism ρ_n is an isomorphism.*

Proof. Let us proceed by induction on n. For $n = 1$, there is a canonical isomorphism $\mathbb{D}/\mathbb{D}_k\mathbf{V} \to k[\mathbf{F}]$ which sends $\mathbf{V}$ to 0 and $w = (\lambda_0, \lambda_1, \dots)$ to λ_0 for all $w \in W(k)$. Hence, the assertion is true by

Lemma 2.2.11. Now, let us assume that ρ_n is an isomorphism and consider the following diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Hom}(\mathbb{G}_a, W_{n+1,k}) & \xrightarrow{\alpha} & \mathrm{Hom}(W_{n+1,k}, W_{n+1,k}) & \xrightarrow{\beta} & \mathrm{Hom}(W_{n,k}, W_{n+1,k}) & \longrightarrow & 0 \\ & & \uparrow i & & \uparrow \rho_{n+1} & & \uparrow \rho_n & & \\ 0 & \longrightarrow & \mathbb{D}\mathbf{V}^n/\mathbb{D}\mathbf{V}^{n+1} & \longrightarrow & \mathbb{D}/\mathbb{D}\mathbf{V}^{n+1} & \longrightarrow & \mathbb{D}/\mathbb{D}\mathbf{V}^n & \longrightarrow & 0. \end{array}$$

The bottom row is exact, so let us consider the top one. The first map is give by $\alpha = (-) \circ \pi_{n,1}$ so it is injective because $\pi_{n,1}$ is an epimorphism. The second map is given by $\beta = (-) \circ \mathcal{I}_n$, so in particular $\beta \circ \alpha = (-) \circ \pi_{n,1} \circ \mathcal{I}_n$ is equal to 0. It remains to prove the surjectivity of β, which follows from Lemma 2.2.14 applied to $j = \mathcal{I}_n$.
By Lemma 2.3.3, $\mathcal{I}_n$ is a morphism of Dieudonné modules hence the square on the right is commutative. Thus, there is a well-defined morphism

$$i\colon \mathbb{D}\mathbf{V}^n/\mathbb{D}\mathbf{V}^{n+1} \longrightarrow \mathrm{Hom}_{(\mathrm{k-\mathbf{Grp}})}(\mathbb{G}_a, W_{n+1,k})$$

which makes the square on the left commute. By the inductive hypothesis, ρ_n is an isomorphism, while β is an isomorphism by Lemma 2.2.13. Therefore, it suffices to prove that i is bijective to conclude that ρ_{n+1} is an isomorphism too.
Let A be a k-algebra, $u \in W_{n+1}(A)$ and $w = (\lambda_0, \lambda_1, \dots) \in W(k)$. Then

$$i(\mathbf{F}^r w \mathbf{V}^n) \circ (\pi_{n,1})(u) = \rho_{n+1}(\mathbf{F}^r w \mathbf{V}^n)(u),$$

so by 2.5 and using the relation $w\mathbf{V}^i = \mathbf{V}^i w^{(p^i)}$, it is equal to

$$F^r_{W_{n+1}(A)}\left(\left(w^{(p^{-n})}\right)_A \cdot (V^n_{W_{n+1}(A)}(u))\right) = F^r_{W_{n+1}(A)} \circ V^n_{W_{n+1}(A)}(w_A \cdot u) =$$
$$F^r_{W_{n+1}(A)} \circ \mathcal{I}_{1,n} \circ \pi_{n,1}(w_A \cdot u) = \mathcal{I}_{1,n} \circ F^r_{\mathbb{G}_a}(\lambda_0 \cdot \pi_{n,1}(u)).$$

Hence, $i(\mathbf{F}^r w \mathbf{V}^n) = \mathcal{I}_{1,n}\rho_1(\mathbf{F}^r \lambda_0)$. Now, the map

$$\mathbb{D}\mathbf{V}^n/\mathbb{D}\mathbf{V}^{n+1}, \quad \mathbf{F}^r w \mathbf{V}^n \longmapsto \mathbf{F}^r \lambda_0$$

is a bijection, ρ_1 is bijective as we remarked above, and finally $\mathcal{I}_{1,n} \circ (-)$ is bijective again by Lemma 2.2.14. Finally, we can conclude that i is an isomorphism. □

2.4 Structure Theorem

In this section, the aim is to apply the preceeding results in order to associate to a commutative unipotent group, which is rather a geometric object, a specific Dieudonné module which is purely algebraic. Let us start by introducing this correspondence, whose definition and properties rely heavily on the theory of Witt groups and their extensions.

2.4.1 Definition of the functor

Let us start by considering the inductive system

$$W_\bullet := \{W_{n,k}, \mathcal{I}_n\colon W_{n,k} \longrightarrow W_{n+1,k}\}_{n\in\mathbb{N}}.$$

By Lemma 2.3.3, this system is compatible with the $\mathbb{D}_k$-module structures.

Definition 2.4.1. Let U be a commutative unipotent k-group. The **Dieudonné module of U** is the left $\mathbb{D}_k$-module

$$\mathcal{M}(U) := \varinjlim_{n \in \mathbb{N}} \mathrm{Hom}_{(\mathrm{k-\mathbf{Grp}})}(U, W_{n,k}).$$

We will denote is as $\mathcal{M}_k(U)$ whenever it is necessary to take the base field into account. Moreover, let us notice that the transition functions of $W_\bullet$ are all monomorphisms so we can identify each

$$\mathcal{M}_n(U) := \mathrm{Hom}_{(\mathrm{k-\mathbf{Grp}})}(U, W_{n,k})$$

with its image in $\mathcal{M}(U)$.
Let $f\colon U \to U'$ be a k-homomorphism between commutative unipotent k-groups. The collection of the natural maps

$$\mathcal{M}_n(f)\colon \mathcal{M}_n(U') \longrightarrow \mathcal{M}_n(U), \quad g \longmapsto g \circ f$$

for all $n \in \mathbb{N}$ is compatible with the inductive limit structure, hence induces a morphism which we will denote as

$$\mathcal{M}(f)\colon \mathcal{M}(U') \longrightarrow \mathcal{M}(U).$$

Notice that for all n, the map $\mathcal{M}_n(f)$ is a $\mathbb{D}/\mathbf{V}^n$-module morphism, hence in particular a $\mathbb{D}$-module morphism. In particular, the limit $\mathcal{M}(f)$ is a morphism of Dieudonné modules.

Remark 2.4.2. Since U is algebraic, there exists an integer n such that $V_U^n = 0$, as seen in Lemma 2.1.13. All maps

$$\mathcal{I}_{n,m} \circ (-)\colon \mathcal{M}_n(U) \longrightarrow \mathcal{M}_{n+m}(U)$$

are bijective, so in particular, the limit $\mathcal{M}(U)$ identifies with $\mathcal{M}_n(U) = \mathrm{Hom}_{(\mathrm{k-\mathbf{Grp}})}(U, W_{n,k})$.
Actually, notice that for all n, $\mathcal{M}_n(U)$ identifies with $\{m \in \mathcal{M}(U)\colon \mathbf{V}^n m = 0\}$. Indeed, if $f\colon U \to W_{n,k}$ is a k-homomorphism, then $V^n_{W_{n,k}} \circ f = 0$. Conversely, let $m \in \mathcal{M}(U)$ such thath $\mathbf{V}^m = 0$: such an element descends to a finite level to a k-homomorphism $h\colon U \to W_{n+q,k}$, such that $V^n_{W_{n+q,k}} \circ h = 0$. Thus, the exact sequence

$$0 \longrightarrow W_{n,k} \xrightarrow{\mathcal{I}_{n,q}} W_{n+1,k} \xrightarrow{V^n_{W_{n+q,k}}} W_{n+q,k}$$

shows that h actually factorizes by $W_{n,k}$ hence m descends to an element in $\mathcal{M}_n(U)$.
In particular, the Dieudonné module associated to an algebraic group satisfies the following definition.

Definition 2.4.3. A Dieudonné module M is said to be **erasable** if for all $m \in M$, there exists an integer $n \geqslant 1$ such that $\mathbf{V}^n m = 0$.

Example 2.4.4. Let us fix $n \geqslant 1$: applying the above remark to $U = W_{n,k}$, we get an isomorphism

$$\Psi_n\colon \mathbb{D}/\mathbb{D}\mathbf{V}^n \xrightarrow{\rho_n} \mathrm{Hom}_{(\mathrm{k-\mathbf{Grp}})}(W_{n,k}, W_{n,k}) = \mathcal{M}_n(W_{n,k}) \xrightarrow{\sim} \mathcal{M}(W_{n,k})$$

of Dieudonné modules.

The discussion above defines a functor

$$\mathcal{M}\colon \{\text{commutative unipotent algebraic groups}\}/k \longrightarrow \{\text{erasable Dieudonné modules of finite type}\}/k.$$

2.4.2 Equivalence of categories

The final result of this chapter is the following theorem, which we now prove, that establishes the equivalence of categories we aimed for. Actually, it holds in a general setting without having to consider the groups to be algebraic : for a more general discussion, see [DG, V, §1].

Theorem 2.4.5 (Structure theorem of commutative unipotent algebraic groups)**.** *The contravariant functor $\mathcal{M}$ is an anti-equivalence of categories between commutative unipotent algebraic groups over k and Dieudonné modules of finite type over k erasable.*

Proof. **Exact** : the functor $\mathcal{M}$ is left exact since all $\mathcal{M}_n = \mathrm{Hom}_{(\mathrm{k-\mathbf{Grp}})}(-, W_{n,k})$ are. It suffices to prove that it is right exact i.e. that it sends monomorphisms to epimorphisms. Let $j\colon U' \to U$ be a closed immersion of algebraic k-groups and consider a composition series of the unipotent quotient U/U' having successive quotients isomorphic to algebraic subgroups of $\mathbb{G}_a$, which exists by Proposition 1.2.5. By taking their inverse images in U', one obtains a sequence of k-subgroups

$$U' = G_0 \subset G_1 \subset \cdots \subset G_r = U$$

such that G_i/G_{i-1} is isomorphic to a k-subgroup of $\mathbb{G}_a$ for all i. Let us proceed by induction on the length r of the composition series: if $r = 1$, setting

$$\varphi\colon U \twoheadrightarrow U/U' = G_1/G_0 \hookrightarrow \mathbb{G}_a,$$

we obtain an exact sequence of the form

$$0 \longrightarrow U' \xrightarrow{j} U \xrightarrow{\varphi} \mathbb{G}_a.$$

Now, let us consider $\mathcal{M}(j)\colon \mathcal{M}(U) \to \mathcal{M}(U')$ and take an element in $\mathcal{M}(U')$, which descends to a k-homomorphism $f \in \mathcal{M}_n(U')$ for a sufficiently large n. By Lemma 2.2.13 there exists $g \in \mathcal{M}_{n+1}(U)$ such that $g \circ j = \mathcal{I}_n \circ f$, which gives a preimage of f in the inductive limit $\mathcal{M}(U)$. Thus, $\mathcal{M}(j)$ is surjective. Now, let $r > 1$ and assume the statement to be true for any k-subgroup admitting such a composition series of length $r-1$. In particular, decomposing the morphism j as

$$j\colon U' \xhookrightarrow{j'} G_{r-1} \xhookrightarrow{j''} U,$$

by the inductive hypothesis both $\mathcal{M}(j')$ and $\mathcal{M}(j'')$ are surjective, hence the same holds for

$$\mathcal{M}(j) = \mathcal{M}(j'' \circ j') = \mathcal{M}(j') \circ \mathcal{M}(j'').$$

Fully faithful : let us fix a commutative unipotent k-group U and consider the map

$$\varphi_{W_{n,k}}\colon \mathrm{Hom}_{(\mathrm{k-\mathbf{Grp}})}(U, W_{n,k}) \longrightarrow \mathrm{Hom}_{\mathbb{D}-\mathrm{mod}}(\mathcal{M}(W_{n,k}), \mathcal{M}(U)), \quad f \longmapsto \mathcal{M}(f).$$

First, $\mathrm{Hom}_{(\mathrm{k-\mathbf{Grp}})}(U, W_{n,k})$ identifies with $\{m \in \mathcal{M}(U)\colon \mathbf{V}^n m = 0\}$ as seen in Remark 2.4.2. On the other hand, by Example 2.4.4 we have

$$\mathrm{Hom}_{\mathbb{D}-\mathrm{mod}}(\mathcal{M}(W_{n,k}), \mathcal{M}(U)) = \mathrm{Hom}_{\mathbb{D}-\mathrm{mod}}(\mathbb{D}/\mathbb{D}\mathbf{V}^n, \mathcal{M}(U)) = \{m \in \mathcal{M}(U)\colon \mathbf{V}^n m = 0\}.$$

Now, let us take H to be any commutative unipotent k-group and fix an exact sequence of the form

$$0 \longrightarrow H \longrightarrow W_{n,k}^r \longrightarrow W_{n,k}^s$$

whose existence is given by Proposition 2.2.15. This induces a commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathrm{Hom}_{(\mathrm{k-}\mathbf{Grp})}(U,H) & \longrightarrow & \mathrm{Hom}_{(\mathrm{k-}\mathbf{Grp})}(U,W_{n,k}^r) & \longrightarrow & \mathrm{Hom}_{(\mathrm{k-}\mathbf{Grp})}(U,W_{n,k}^s) \\ & & \downarrow \varphi_H & & \downarrow \varphi_{W_{n,k}^r} & & \downarrow \varphi_{W_{n,k}^s} \\ 0 & \longrightarrow & \mathrm{Hom}_{\mathbb{D}}(\mathcal{M}(H),\mathcal{M}(U)) & \longrightarrow & \mathrm{Hom}_{\mathbb{D}}(\mathcal{M}(W_{n,k}^r),\mathcal{M}(U)) & \longrightarrow & \mathrm{Hom}_{\mathbb{D}}(\mathcal{M}(W_{n,k}^s),\mathcal{M}(U)). \end{array}$$

Since $\varphi_{W_{n,k}^r}$ and $\varphi_{W_{n,k}^s}$ are both bijective, we obtain that φ_H is bijective too.

Essentially surjective : Let M be a Dieudonné module of finite type and erasable. In particular, there exists an integer $n \geqslant 1$ such that $\mathbf{V}^n M = 0$, so it has a natural structure of $\mathbb{D}/\mathbb{D}\mathbf{V}^n$-module. Since the ring $\mathbb{D}/\mathbb{D}\mathbf{V}^n$ is noetherian (see [DG, V, §1, 3.2]), a module of finite type is of finite presentation, hence there exist integers r, s and an exact sequence

$$(\mathbb{D}/\mathbb{D}\mathbf{V}^n)^s \xrightarrow{\varphi} (\mathbb{D}/\mathbb{D}\mathbf{V}^n)^r \longrightarrow M \longrightarrow 0.$$

By full faithfulness of the functor $\mathcal{M}$, there exists a k-homomorphism $f\colon W_{n,k}^r \longrightarrow W_{n,k}^s$ such that $\varphi = \mathcal{M}(f)$, so by exactness of $\mathcal{M}$, the exact sequence

$$0 \longrightarrow \ker f \longrightarrow W_{n,k}^r \xrightarrow{f} W_{n,k}^s$$

implies that $M \simeq \mathcal{M}(\ker f)$. □

Proposition 2.4.6. *Let K/k be a perfect field extension of k and U a commutative unipotent k-group. Then there exists a canonical isomorphism*

$$W(K) \otimes_{W(k)} \mathcal{M}(U) \xrightarrow{\sim} \mathcal{M}(U_K).$$

Proof. See [DG, V, §1, 4.9] □

Example 2.4.7. Let us see what the above equivalence of categories looks like in some of the simplest commutative unipotent groups.

- Example 2.4.4 shows that $\mathcal{M}(W_{n,k})$ identifies with $\mathbb{D}/\mathbb{D}\mathbf{V}^n$, the simplest case being

$$\mathcal{M}(\mathbb{G}_a) = \mathcal{M}_1(\mathbb{G}_a) = \mathbb{D}/\mathbb{D}\mathbf{V} = k[\mathbf{F}] = \mathrm{End}(\mathbb{G}_a).$$

- Setting $W_{m,n} := \ker(F^i_{W_{n,k}}\colon W_{n,k} \to W_{n,k})$, the theorew gives

$$\mathcal{M}(W_{m,n}) = \mathbb{D}/\left(\mathbb{D}\mathbf{F}^m + \mathbb{D}\mathbf{V}^n\right);$$

  again, the easiest case is obtained by setting $n = 1$:

$$\mathcal{M}(W_{m,1}) = \mathcal{M}(\alpha_{p^m}) = \mathbb{D}/\left(\mathbb{D}\mathbf{F}^m + \mathbb{D}\mathbf{V}\right) = k[\mathbf{F}]/(\mathbf{F}^m).$$

- By using the Artin-Schreier exact sequence

$$0 \longrightarrow (\mathbb{Z}/p^n\mathbb{Z})_k \longrightarrow W_{n,k} \xrightarrow{\mathbf{F}-\mathrm{id}} W_{n,k} \longrightarrow 0$$

  one concludes by exactness of $\mathcal{M}$ that

$$\mathcal{M}\left(\mathbb{Z}/p^n\mathbb{Z}\right) = \mathbb{D}/\left(\mathbb{D}\mathbf{V}^n + \mathbb{D}(\mathbf{F}-1)\right).$$

Why imperfect fields?

This short chapter constitutes a link between the theory over perfect field and arbitrary, most of the time imperfect, ones: first, it shows that the vanishing of the unipotent radical is not a geometric property. It continues by illustrating Rosengarten's rigidity result, which gives an interesting motivation to the study of wound unipotent groups.

3.1 Preliminaries : Weil restriction

The restriction of scalars is an elementary construction in the theory of algebraic groups, playing at the same time a fundamental role, because it gives rise to interesting examples and it is used to construct the so called standard pseudo-reductive groups. Here, it will be used in some proofs and examples.

Throughout this subsection, let K denote a finite k-algebra : the notation K is due to the fact that in most cases this is applied to a finite field extension K/k. Also, recall that we are restricting to the affine case.

Proposition 3.1.1. *Let G be an algebraic group over K. The functor*

$$\mathcal{R}_{K/k}(G)\colon (\mathrm{k}-\mathbf{Alg}) \longrightarrow (\mathbf{Set}), \quad R \longmapsto G(K \otimes R)$$

is group-valued and represented by an affine scheme of finite type over k, hence it is an algebraic group.

Proof. Let $G = \operatorname{Spec} A$. Since it is of finite type, there exists suitable integers $d, m \in \mathbb{N}$ and polynomials $f_i \in K[X_1, \dots, X_d]$ such that

$$A \simeq K[X_1, \dots, X_d]/(f_1, \dots, f_m).$$

Let $e_1, \dots, e_n$ be a basis of K as a k-vector space and set

$$X_i := Y_{i1}e_1 + \dots + Y_{in}e_n = \sum_j Y_{ij}e_j,$$
$$f_h := g_{h1}e_1 + \dots + g_{hn}e_n = \sum_l g_{hl}e_l.$$

for all $i = 1, \dots, d$ and $h = 1, \dots, m$. An element of $\mathcal{R}_{K/k}(G) = G(K \otimes R) = \operatorname{Hom}_{(\mathrm{k}-\mathbf{Alg})}(A, K \otimes R)$ is given by a morphism

$$\varphi\colon K[X_1, \dots, X_d]/(f_1, \dots, f_m) \longrightarrow K \otimes R$$
$$\overline{X_i} \longmapsto \sum_j e_j \otimes r_{ij},$$

where $\overline{X_i}$ denotes the image ot X_i in A. This induces a k-algebra homomorphism

$$\begin{aligned} \varphi' \colon B := k[Y_{ij}, 1 \leqslant i \leqslant d, 1 \leqslant j \leqslant n]/(g_{hl}, 1 \leqslant h \leqslant m, 1 \leqslant l \leqslant n) &\longrightarrow R \\ \overline{Y_{ij}} &\longmapsto r_{ij}. \end{aligned}$$

The map $\varphi \mapsto \varphi'$ gives a bijection $\mathrm{Hom}_{(\mathrm{K-\mathbf{Alg}})}(A, K \otimes R) \simeq \mathrm{Hom}_{(\mathrm{k-\mathbf{Alg}})}(B, R)$, so we have proved that $\mathcal{R}_{K/k}(G)$ is represented by $\operatorname{Spec} B$. For a more general statement and proof, see [BLR12, 7.6]. □

Definition 3.1.2. Let G be an algebraic group over K. The algebraic group $\mathcal{R}_{K/k}(G)$ over k is called the **Weil restriction** or the **restriction of scalars** of G.

This defines a functor

$$\mathcal{R}_{K/k} \colon (\mathrm{K} - \mathbf{Grp}) \longrightarrow (\mathrm{k} - \mathbf{Grp}), \quad G \longmapsto \mathcal{R}_{K/k}(G).$$

Now let us consider the homomorphism defined on the functor of points as the natural transformation

$$\begin{cases} i_G \colon & G \hookrightarrow \mathcal{R}_{K/k}(G_K) \\ & G(R) \longrightarrow G(K \otimes R), \end{cases}$$

induced by the k-algebra morphism $R \to K \otimes R$, $r \mapsto 1 \otimes r$, for all k-algebra R. This is a monomorphism of algebraic groups, hence a closed immersion (see [Mil17, Theorem 5.34]). This canonical mapping has the following universal property.

Proposition 3.1.3. *Let G be an algebraic group over k and H an algebraic group over K. For every k-homomorphism*

$$\alpha \colon G \longrightarrow \mathcal{R}_{K/k}(H),$$

there exists a unique K-homomorphism $\beta \colon G_K \to H$ such that the following diagram commutes:

$$\begin{array}{ccccc} G & \xrightarrow{\;i_G\;} & \mathcal{R}_{K/k}(G_K) & \qquad & G_K \\ & \searrow^{\alpha} & \downarrow{\scriptstyle \mathcal{R}_{K/k}(\beta)} & & \downarrow{\scriptstyle \exists!\beta} \\ & & \mathcal{R}_{K/k}(H) & & H \end{array}$$

Remark 3.1.4. The universal property above can be expressed by an adjunction as follows : for all algebraic group G over k and H over K, there is a bijection

$$\mathrm{Hom}_{(\mathrm{k-\mathbf{Grp}})}(G, \mathcal{R}_{K/k}(H)) \xrightarrow{\sim} \mathrm{Hom}_{(\mathrm{K-\mathbf{Grp}})}(G_K, H).$$

The functor $\mathcal{R}_{K/k}$ is therefore right adjoint to the base change functor $G \mapsto G_K$. An important consequence is that it is left exact, thus it preserves inverse limits, such as kernels, products and fiber products.

Proof. Giving an adjunction between two functors $\mathbf{F} \colon \mathcal{A} \to \mathcal{B}$ (on the left) and $\mathbf{G} \colon \mathcal{B} \to \mathcal{A}$ (on the right) is equivalent to giving a couple of natural transformations

$$\eta \colon \mathbf{1}_{\mathcal{A}} \longrightarrow \mathbf{GF}, \quad \varepsilon \colon \mathbf{FG} \longrightarrow \mathbf{1}_{\mathcal{B}},$$

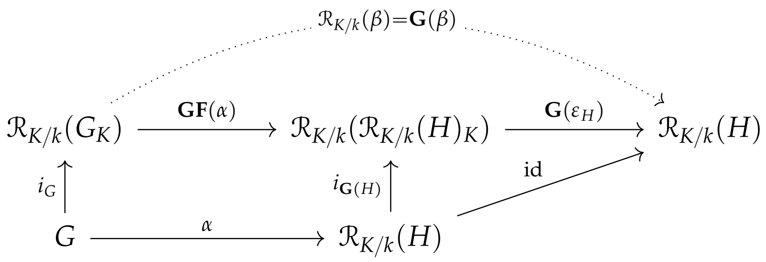
called respectively unit and counit of the adjunction, such that the following triangle identities hold for all $A \in \mathcal{A}$ and $B \in \mathcal{B}$:

$$\varepsilon_{\mathbf{F}(A)} \circ F(\eta_A) = \mathrm{id}_{\mathbf{F}(A)}, \quad \mathbf{G}(\varepsilon_B) \circ \eta_{\mathbf{G}(B)} = \mathrm{id}_{\mathbf{G}(B)}\,. \tag{3.1}$$

For more details, see [Lei14, §2.2].
In our case, $\mathbf{F}\colon (\mathrm{k}-\mathbf{Grp}) \to (\mathrm{K}-\mathbf{Grp})$ is the base change functor, $\mathbf{G}\colon (\mathrm{K}-\mathbf{Grp}) \to (\mathrm{k}-\mathbf{Grp})$ is the Weil restriction. The morphism i_G described above is functorial in G and defines the unit of the adjonction. Now, let us consider a K-algebra R' and denote it as R'_0 when it is regarded as a k-algebra via the morphism $k \to K \to R'$. There is a natural K-algebra morphism $K \otimes R'_0 \to R'$, sending $\lambda \otimes r \mapsto \lambda r$, which induces a morphism

$$\varepsilon_H\colon \left(\mathcal{R}_{K/k}(H)\right)_K \longrightarrow H, \quad H(K \otimes R'_0) \longrightarrow H(R').$$

This is functorial in H and defines the counity of the adjunction. Since the triangle identities hold, the morphism $\mathcal{R}_{K/k}(\beta)$ is given by the following diagram.



The left hand square commutes by functoriality of i, while the right hand triangle expresses the second identity in 3.1. □

The intuition behind the idea of Weil restriction might lead to think that, for a finite extension k'/k, the k-group structure of $\mathcal{R}_{k'/k}(G_{k'})(R)$ is similar to the one of $G^{[k'\colon k]}$. This holds for the additive group, but in general it is far from being true, as illustrated by the following example.

Example 3.1.5. Let k be an imperfect field of characteristic $p = 2$ and $t \in k \backslash k^2$. Consider the purely inseparable extension $k' = k(\sqrt{t})$ and the algebraic group $G := \mathcal{R}_{k'/k}(\mathbb{G}_{m,k'})$, obtained by Weil restriction of the multiplicative group. For any k-algebra R,

$$G(R) := \mathcal{R}_{k'/k}(\mathbb{G}_{m,k'})(R) = \mathbb{G}_{m,k'}(k' \otimes R) = (k' \otimes R)^\times = \{x + y\sqrt{t},\ x^2 - ty^2 \in R^\times\},$$

because an element $x + y\sqrt{t} \in k' \otimes R = R \oplus \sqrt{t}R$ is inversible if and only if the R-linear map

$$\begin{pmatrix} a \\ b \end{pmatrix} \simeq a + b\sqrt{t} \longmapsto (a + b\sqrt{t})(x + y\sqrt{t}) = ax + byt + (bx + ay)\sqrt{t} \simeq \begin{pmatrix} x & ty \\ y & x \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}$$

which is true if and only if its determinant $x^2 - ty^2$ is invertible. As a set, the abstract group $G(R)$ identifies with $\mathbb{G}^2_{m,k}(R) = \{(x,y) \in R^2\colon x^2 - ty^2 \in R^\times\}$. However, the group law in $G(R)$ is given by

$$(x,y) * (x',y') = (x + y\sqrt{t})(x' + y'\sqrt{t}) = (xx' + tyy' + (xy' + x'y)\sqrt{t}),$$

hence it is not the same as the one in $\mathbb{G}^2_{m,k}(R)$. Moreover, this group is one of the simplest examples of a pseudo-reductive group which is not reductive, as we will see in Example 3.2.3 below.

In the case of a separable field extension, the process of Weil restriction behaves in a much simpler way : it is analogous to the idea of viewing a complex manifold of dimension n as a real manifold of dimension $2n$. More precisely, we have the following result.

Proposition 3.1.6. *Let k'/k be a finite separable field extension and K/k a finite Galois extension that splits k'/k. For an algebraic group G over k', there is an isomorphism*

$$\left(\mathcal{R}_{k'/k}(G)\right)_K \simeq \prod_{\sigma\colon k'\hookrightarrow K} G \times_{\operatorname{Spec} k',\sigma} \operatorname{Spec} K,$$

where σ runs over all embeddings $k' \hookrightarrow K$.

Proof. See [Mil17, 2.61]. □

3.2 Pseudo-reductivity

As mentioned before, the first reason behind the study of unipotent groups over imperfect fields is that pseudo-reductivity cannot be verified on the algebraic closure, because the unipotent radical of a smooth connected algebraic group can become larger after a purely inseparable extension of scalars on the base field. Let us start by giving precise definitions reductivity and pseudo-reductivity.

Let G be a smooth connected algebraic group over k. Let us recall that its unipotent radical $R_{u,k}(G)$ is defined to be its largest smooth connected unipotent normal k-subgroup (see Corollary 1.1.12).

Definition 3.2.1. A smooth connected k-group G is **reductive** if its geometric unipotent radical $R_{u,\bar{k}}(G_{\bar{k}})$ is trivial, and it is **pseudo-reductive** if $R_{u,k}(G)$ is trivial.

The following key result states that the unipotent radical commutes with a separable extension of scalars : in particular, over a perfect field the notion of reductive and pseudo-reductive coincide.

Theorem 3.2.2. *Let K/k be a* ***separable*** *field extension and G a smooth connected affine k-group. Then*

$$R_{u,k}(G)_K = R_{u,K}(G_K).$$

In other terms, the formation of the unipotent radical commutes with separable extensions of the ground field. In particular, G is ***pseudo-reductive*** *over k if and only if it is pseudo-reductive over K.*

Proof. Since $R_{u,k}(G)_K$ is a smooth connected normal unipotent subgroup of G_K, the inclusion $R_{u,k}(G)_K \subseteq R_{u,K}(G_K)$ always holds. First, we claim that we can restrict to the case of a separably closed base field k. For that, let us start by considering a Galois extension k'/k: by Galois descent, $R_{u,k'}(G_{k'})$ descends to a smooth connected unipotent normal k-subgroup $H \subset G$, which is by definition contained in $R_{u,k}(G)$. Hence $R_{u,k'}(G_{k'}) = H_{k'} \subseteq R_{u,k}(G)_{k'}$ and we are done. Now let k_s/k and K_s/K be separable closures, chosen such that $k_s \subseteq K_s$. Both k_s/k and K_s/K are Galois, hence

$$\alpha\colon R_{u,k}(G)_{k_s} \longrightarrow R_{u,k_s}(G_{k_s})$$
$$\beta\colon R_{u,K}(G)_{K_s} \longrightarrow R_{u,K_s}(G_{K_s})$$

are isomorphisms. If we denote by i the inclusion $R_{u,k}(G)_K \to R_{u,K}(G_K)$, the following diagram commutes:

$$\begin{array}{ccc} R_{u,k_s}(G_{k_s})_{K_s} & \xrightarrow[\gamma]{} & R_{u,k_s}(G_{K_s}) \\ \uparrow{\scriptstyle \alpha\otimes K_s} & & \uparrow{\scriptstyle \beta} \\ (R_{u,k}(G)_{k_s})_{K_s} = (R_{u,k}(G)_K)_{K_s} & \xrightarrow{i\otimes K_s} & R_{u,K}(G_K)_{K_s} \end{array}$$

If γ is an isomorphism, then the same is true for $i \otimes K_s$. By Galois descent, this implies that i is an isomorphism. Therefore it suffices to prove the theorem for k a separably closed field.

Now, the inclusion we want to prove is $R_{u,K}(G_K) \subset R_{u,k}(G)_K$. Since they are both smooth and connected subgroups, it suffices to prove an inequality on dimensions. Actually, we will prove the following more general fact : let $U \subset G_K$ be a smooth connected unipotent normal K-subgroup with $\dim U = d$, then from U we can construct a smooth connected unipotent normal k-subgroup of G having dimension d. For this, we express K as the direct limit $K = \varinjlim F$ of all its subfields $k \subseteq F \subseteq K$ which are finitely generated over k Since K/k is separable, let us note that each F is necessarily separable over k. Based on descent of closed subschemes and morphisms between them, as in [EGA4, Prop 8.6.3 and 8.9.1], there exists such an F for which U descends to an F-subgroup of G_F. Let U_0 be such a subgroup: since $(U_0)_K = U$, by faithfully flat descent U_0 is necessarily smooth, connected, unipotent and normal in G_F (to prove it we do not need the results on inductive limits). By replacing K by F, this allows to suppose that the extension K/k is finitely generated. Therefore it must be of the form

$$k \hookrightarrow k(X_1, \ldots, X_m) \hookrightarrow K$$

where the first is purely transcendental and the second is finite and separable, hence by the primitive element theorem it is monogeneous: there exists $\alpha \in K$ such that it is an extension of the form $K = k(X_1, \ldots, X_m)(\alpha) = k(X_1, \ldots, X_m)[T]/(P)$, where $P \in k(X_1, \ldots, X_m)[T]$ is a separable polynomial. By replacing α by a suitable $f\alpha$ with $f \in k[X_1, \ldots, X_m]$ we can suppose that P is a polynomial with coefficients in $k[X_1, \ldots, X_m]$. Hence

$$K = k(X_1, \ldots, X_m)[T]/(P) = \mathrm{Frac}\,(k[X_1, \ldots, X_m]/(P)) =: \mathrm{Frac}(A).$$

Now, let us express K as the following direct limit

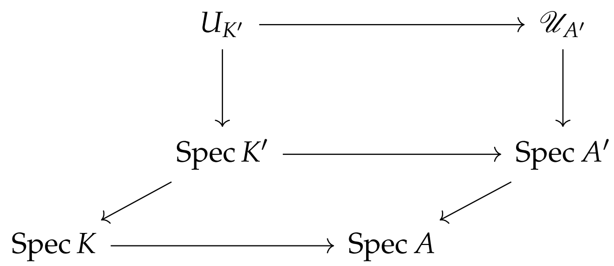
$$K = \mathrm{Frac}\,A = A_{(0)} = \varinjlim_{a \in A \setminus \{0\}} A[1/a]$$

By separability of P, we can obtain that the morphism $\mathrm{Spec}\,A \to \mathrm{Spec}\,k$ is smooth, i.e. A is a k-smooth domain, after replacing $\mathrm{Spec}\,A$ by some open subscheme $\mathrm{Spec}\,A[1/a]$. Again by standard results on limits, there exists a suitable localisation $A[1/a]$ such that U descends to a closed subscheme of $G_{A[1/a]}$: by replacing A with this localisation, there exists a closed subscheme $\mathscr{U} \subseteq G_A$ such that $\mathscr{U}_K = U \subseteq G_K$.

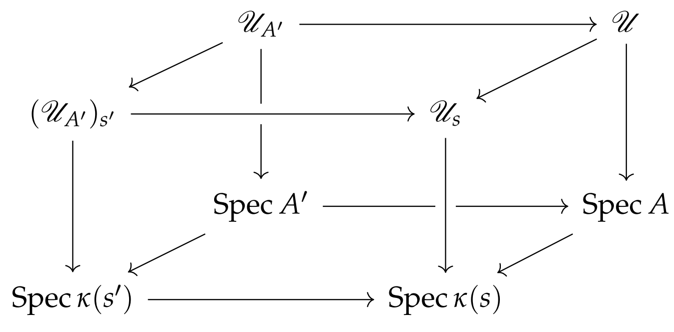
Now we want to prove that, by further remplacing A by a localisation, we can suppose that $\mathscr{U}$ is a unipotent normal A-subgroup of G_A. This is done by "spreading out" these properties from the generic fiber $\mathrm{Spec}\,K$. The normality of U in G_K is equivalent to saying that the map

$$G_K \times U \to G_K, \quad (g, u) \mapsto gug^{-1}$$

factors through U. Therefore it suffices to apply descent of morphisms from $K = \varinjlim A[1/a]$ to obtain that $\mathscr{U}$ is an A-smooth normal A-subgroup of G_A, having geometrically connected fibers of dimension d, because U_K is the generic fiber of $\mathscr{U} \to \operatorname{Spec} A$. Geometrically, remplacing A by $A[1/a]$ corresponds to shrinking $\operatorname{Spec} A$ by taking out the hypersurface $(a = 0)$. Concerning the unipotence of U_K, by Corollary 1.2.6 it can be expressed as follows: there exists a finite extension K'/K such that $U_{K'}$ admits a composition series whose successive quotients are isomorphic to $\mathbb{G}_{a,K'}$. Let $\alpha_1, \ldots, \alpha_n$ a K-basis of K' and set $A' := A[\alpha_1, \ldots, \alpha_n]$. Then A' is an A-finite domain such that $A'_K = K'$. Let us consider the following commutative diagram, which is by construction made up of cartesian squares given by fiber products:



The field extension $K \to K'$ is faithfully flat, so up to restricting A to a localization we obtain that $A \to A'$ is faithfully flat too. Moreover, the diagram shows that the generic fiber of $\operatorname{Spec} A' \to \operatorname{Spec} A$ is $\operatorname{Spec} K'$. Since it is true for $U_{K'}$, by spreading out of properties as before, from this diagram we can suppose that $\mathscr{U}_{A'}$ admits a composition series by A'-smooth normal closed A-subgroups, having successive quotients isomorphic to $\mathbb{G}_{a\,A'}$.
As a final step, we claim that all fibers of $\mathscr{U} \to \operatorname{Spec} A$ are unipotent. Suppose this is true: since A is k-smooth and k separably closed, $A(k)$ is dense in A, hence there exists a k-point of $\operatorname{Spec} A$. The fiber of $\mathscr{U}$ over such a point is a normal k-subgroup of G which is smooth, connected, unipotent and of dimension precisely d.
To prove it, let us fix a point $s \in \operatorname{Spec} A$, which corresponds to a morphism $\operatorname{Spec} \kappa(s) \to \operatorname{Spec} A$. Since $\operatorname{Spec} A' \to \operatorname{Spec} A$ is faithfully flat, in particular it is surjective, so there exists $s' \in \operatorname{Spec} A'$ a preimage of s. Let us consider the following commutative diagram :



where we denote the fibers over s and s' as

$$\mathscr{U}_s := \mathscr{U} \otimes_A \kappa(s)$$
$$(\mathscr{U}_{A'})_{s'} := (\mathscr{U}_{A'}) \otimes_{A'} \kappa(s')$$

The commutative square in the front tells us that $(\mathscr{U}_{A'})_{s'} = \mathscr{U}_s \otimes_{\kappa(s)} \kappa(s')$. Since being unipotent commutes with extensions of the base field (Corollary 1.1.12), this implies that $\mathscr{U}_s$ is unipotent. □

Theorem 3.2.2 fails when purely inseparable field extensions are taken into account, as illustrated by the following example : it is the simplest case of a pseudo-reductive nonreductive algebraic group and it is a generalization of Example 3.1.5 above.

Example 3.2.3. Let k be an imperfect field of characteristic $p > 0$ and k'/k a purely inseparable field extension of degree $[k' : k] = p^n$. Let us consider the smooth k-group G, obtained by Weil restriction of the multiplicative group:

$$G := \mathcal{R}_{k'/k}(\mathbb{G}_{m,k'}).$$

The group $\mathbb{G}_{m,k}$ embeds as a k-subgroup of G, as we have seen in Defintiion 3.1.2. Hence, we can consider the quotient $U := G/\mathbb{G}_m$. The smoothness of G comes from the following general property of Weil restriction : if Y is a smooth k'-variety, then $\mathcal{R}_{k'/k}(Y)$ is smooth over k. First, we claim that there exists an integer n such that $U^{p^n} = 1$. By smoothness of U, it suffices to verify that this is true for $U(k_s)$, because k_s-rational points are schematically dense. Thus, we compute

$$U(k_s)^{p^n} = \left(\mathbb{G}_m(k' \otimes_k k_s)/\mathbb{G}_m(k_s)\right)^{p^n} = \left((k' \otimes_k k_s)^\times / k_s^\times\right) = 1,$$

because k'/k is purely inseparable and k_s/k is separable, so their tensor product over k is a field.
Next, we claim that if a k-group H is not unipotent, then it contains a one-dimensional torus T. (question need borel subgroups...?)
Now, we want to apply this in order to show that U is unipotent. If this is not true, then it must admit a one-dimensional torus T as a k-subgroup, which we can assume to be split by extending scalars to k_s. Hence, for all $m \geqslant 1$, $T = T^{p^m}$ because the sequence

$$1 \longrightarrow \mu_{p^m} \longleftrightarrow \mathbb{G}_m \xrightarrow{p^n \cdot} \mathbb{G}_m \longrightarrow 1$$

is exact. This contradicts the fact that $U^{p^n} = 1$, hence the quotient U is unipotent. In particular, the k-group G is not reductive.
On the other hand, we have

$$G(k_s) = (k' \otimes_k k_s)^\times$$

which has no p^n-torsion for any n since $k' \otimes_k k_s$ is a field. In particular, it does not contain any unipotent subgroup (normal or not), so by density of the rational points the same holds for the algebraic group G_{k_s}. Thus, $R_{u,k_s}(G_{k_s})$ is trivial, hence the unipotent radical $R_{u,k}(G)$ is trivial too and we have shown that G is pseudo-reductive.

The above argument can be generalized as follows : if k'/k is a finite purely inseparable extension and G' is a smooth connected nontrivial reductive k'-group, then the Weil restriction

$$G := \mathcal{R}_{k'/k}(G')$$

is not reductive, even though it is pseudo-reductive (see [CGP15, Example 1.6.1]).

3.3 Rigidity for Unirational Groups

Throughout the preceding sections it has been shown that, when working with unipotent or pseudo-reductive groups, purely inseparable extensions lead to many complications that do not take place in the separable case. Moreover, in the last chapter we have established and explained an equivalence of categories, which only holds in the commutative case and over a perfect field. So, why the need to study groups over imperfect fields?
The first reason is that, whenever one does algebraic geometry over a perfect field k of nonzero characteristic, the fiber over the generic point of any smooth k-variety, its function field, is always imperfect. The simplest class of imperfect fields are those such that $[K^{1/p}\colon K] = p$, also called of degree of imperfection 1. Geometrically, such a field K is the function field of some smooth k-curve. Some examples include $\mathbb{F}_p(t)$, $\mathbb{F}_p(\!(t)\!)$ and more generally all global and local fields of nonzero characteristic (for basics on global and local fields see [Neu13, *II*, §5]).

However, interesting stimuli exist already within the theory of algebraic groups : over an imperfect field, groups have a more rich and complex structure, and this is particularly true for unipotent ones. Let us mention and give a few comments on a rigidity result which is an application of Tits' theory.

First, over a perfect field k, each smooth connected nontrivial unipotent group U contains a copy of the additive group. Notice that this makes it impossible to have a rigidity theorem for scheme maps $f\colon G \to U$ satisfying $f(1_G) = 1_U$, analogous to the usual fundamental rigidity theorem for abelian varieties. For example, one can define a counterexample as

$$f\colon \mathbb{G}_m \xrightarrow{\;g\;} \mathbb{G}_a \hookrightarrow U,$$

where $g(x) = x - 1$: clearly, f is a k-scheme morphism satisfying $f(1_{\mathbb{G}_m}) = 1_U$, but it is not a k-group homomorphism.

On the other hand, over imperfect fields there exist several smooth and connected unipotent groups that do not contain any copy of $\mathbb{G}_a$ (the simplest one being Example 4.1.2 below): this makes a big difference, as the following recent result, which is still to appear in the literature, shows.

Theorem 3.3.1 (Rosengarten)**.** *Let G and H be group schemes of finite type over a field k of degree of imperfection* 1*. Assume that G is unirational and that H is solvable and does not contain a k-subgroup isomorphic to $\mathbb{G}_a$. Then any k-scheme morphism $f\colon G \longrightarrow H$ such that $f(1_G) = 1_H$ is a homomorphism of k-group schemes.*

Let us recall that a k-variety is said to be **unirational** if there exists an integer $N \geqslant 1$ and a rational map $\mathbb{P}^N \dashrightarrow X$; essentially, this is a useful property to guarantee the existence of many rational points. In characteristic 0, and more generally over a perfect base field, all affine algebraic groups are unirational, hence the first assumption is non tautological only when working over an imperfect field.

What about the second assumption? It involves solvable groups not containing a copy of $\mathbb{G}_a$: in particular, in this text we will study the case of unipotent groups, which Tits calls ***k*-wound**.
In order to state the theorem, the precise definition of this notion is not needed; however, it is heavily used in the proof given by Rosengarten. Again, if the base field is perfect, this condition is not

satisfied by any nontrivial smooth connected unipotent group, hence the rigidity theorem actually makes sense only over an imperfect base field.

An important consequence is given by the following corollary, which follows directly from the theorem by taking $G = H$ a unipotent wound group and applying the statement to the inversion map, as one does in the case of abelian varieties.

Corollary 3.3.2. *Let k be a field of degree of imperfection* 1*. Then any unirational wound unipotent k-group is commutative.*

Tits' work on wound groups

This last chapter follows [CGP15, Appendix B], and [Con11]. Even though a complete exposition of Tits' results has only been published in [CGP15], most of the material can be found in his unpublished Yale lecture notes from 1967.
The intent is to survey Tits' work on the structure of smooth connected unipotent groups over an arbitrary field, in particular concerning the imperfect case. This involves introducing and studying the k-wound property, concluding with some results on the actions of tori on unipotent groups, which are useful to proceed further on with the study of general solvable groups. Particular attention is paid to illustrate a few examples in detail, in order to highlight the differences with the perfect case and the pathologies which might arise.
Henceforth, k will denote an arbitrary field of characteristic $p > 0$.

4.1 Subgroups of vector groups

Recall that a smooth solvable k-group is ***k*-split** if it admits a composition series having successive quotients isomorphic to $\mathbb{G}_a$ or $\mathbb{G}_m$. For k-tori, this notion behaves in a very convenient manner: all subgroups and quotients of a k-split torus are k-split. Moreover, the notion of ***k*-anisotropicity** is orthogonal to the k-split property, as in the following result (see [Bor91, 8.14 and 8.15]).

Proposition 4.1.1. *Let T be a torus over k. Then there exist a unique maximal k-split subtorus T_s and a unique maximal k-anisotropic subtorus T_a, such that the mapping*

$$T_a \times T_s \longrightarrow T, \quad (a, s) \longmapsto as$$

is an isogeny.

What changes when we move on to the unipotent case? First, the following example shows that a smooth connected normal k-subgroup of a k-split unipotent group is not necessarily k-split.

Example 4.1.2. Let k be imperfect and $a \in k \backslash k^p$. Consider the k-split unipotent group $\mathbb{G}_a^2$ and the k-subgroup $U \subset \mathbb{G}_a^2$ defined on the functor of points as

$$U(R) := \{(x, y) \in R^2 \colon y^p = x - ax^p\}$$

for all k-algebras R, i.e.

$$U = \operatorname{Spec}\left(\frac{k[X, Y]}{(Y^p - X + aX^p)}\right).$$

Now let $k' := k(a^{1/p})$: if we extend scalars to k', the group $U_{k'}$ is isomorphic to $\mathbb{G}_a$, hence in particular it is k'-split:

$$U_{k'} = U \times_{\operatorname{Spec} k} \operatorname{Spec} k' = \operatorname{Spec}\left(\frac{k[X,Y]}{(Y^p - X + aX^p)} \otimes_k k'\right) = \operatorname{Spec}\left(\frac{k'[X,Y]}{(Y^p - X + (a^{1/p}X)^p)}\right)$$
$$= \operatorname{Spec}\left(\frac{k'[X,Y]}{((Y - a^{1/p}X)^p - X)}\right) \simeq \operatorname{Spec}\left(\frac{k'[V,T]}{(T^p - V)}\right) \simeq \operatorname{Spec} k'[T] = (\mathbb{G}_a)_{k'}$$

However, U is not isomorphic to $\mathbb{G}_a$ as a k-scheme, hence in particular it is not k-split as a k-group. Let us assume that $\mathcal{O}(U) = k[X,Y]/(Y^p - X + aX^p)$ and $k[T]$ are isomorphic as a k-algebras. Let us denote x and y the images of X and Y in the quotient $\mathcal{O}(U)$: the isomorphism gives $x = Q(T)$, $y = R(T)$ for suitable polynomials $Q, R \in k[T]$ of degree strictly larger than 1. Moreover, the equality $y^p = x - ax^p$ implies that Q and R have same degree. Thus, we obtain

$$Q^p(T) = R(T) - aR(T)^p \in k[T].$$

Considering the highest degree term on both sides, this gives $a \in k^p$, which is absurd.

This example also shows that the k-split property for unipotent groups can be sensitive to purely inseparable extensions, unlike what happens in the case of groups of multiplicative type (see [Mil17], Corollary 12.20).

Carrying on the comparison with the case of tori, we wish to define and study an analogue for unipotent k-groups of the notion of k-anisotropicity. Let us start by a preliminary study of subgroups of vector groups, which are in particular unipotent, commutative and p-torsion. The aim of this first section is to show that any such unipotent group embeds into a vector group, and to establish the conditions under which the embedding can be realized in codimension 1.

4.1.1 p-polynomials

Definition 4.1.3. A polynomial $f \in k[X_1, \dots, X_n]$ is a **p-polynomial** if every monomial appearing in f is of the form $c_{ij} X_i^{p^j}$ for some $i \in \{1 \dots n\}$, $j \in \mathbb{N}$ and $c_{ij} \in k$.

In particular, remark that $f = \sum_{i=1}^n f_i(X_i)$ where $f_i(X_i) = \sum_j c_{ij} X_i^{p^j} \in k[X_i]$. The polynomials f_i are uniquely determined if we add the condition $f_i(0) = 0$ for all i.

Lemma 4.1.4. *A polynomial $f \in k[X_1, \dots, X_n]$ is a p-polynomial if and only if the associated map of k-schemes $\mathbb{G}_a^n \to \mathbb{G}_a$ is a k-homomorphism.*

Proof. We associate to f in a natural way the map $\mathbb{G}_a^n \to \mathbb{G}_a$ given on the functor of points by

$$\mathbb{G}_a^n(R) = R^n \longrightarrow R = \mathbb{G}_a(R), \quad x = (x_1, \dots, x_n) \longmapsto f(x_1, \dots, x_n)$$

for all k-algebras R.

- Let f be a p-polynomial, then it is of the form $f = \sum_{i,j} c_{ij} X_i^{p^j}$. For all $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n) \in R^n$, we clearly have

$$f(x+y) = \sum_{i,j} (x_i + y_i)^{p^j} = \sum_{i,j} x_i^{p^j} + \sum_{i,j} y_i^{p^j} = f(x) + f(y),$$

  hence the map is a k-homomorphism.

- We proceed by induction on the number n of indeterminates. For $n = 1$, the polynomial $g(X, Y) := f(X+Y) - f(X) - f(Y)$ is zero in $k[X, Y]$. Write f as $f = \sum_{k=1}^{m} a_l X^l$ for some $a_l \in k$. Then

$$0 = g(X, Y) \sum_{l=0}^{m} a_l ((X+Y)^l - X^l - Y^l)$$

thus whenever $a_l \neq 0$ it must be $(X+Y)^l = X^l + Y^l$, which is true if and only if $l = p^j$. We conclude by setting $c_j := a_{p^j}$. Now suppose the statement true for n and consider $f \in k[X_1 \ldots, X_n, T]$ which is additive. Write it as

$$f(X, T) = g_0(X) + g_1(X)T + \ldots + g_m(X)T^m \in k[X_1, \ldots, X_n][T]$$

In particular, $g_0(X+Y) = f(X+Y, 0) = f(X, 0) + f(Y, 0) = g_0(X) + g_0(Y)$, hence by induction g_0 is a p-polynomial. It suffices to prove that $g_1, \ldots, g_m \in k[X-1, \ldots, X_n]$ are constant : this implies $f(X, T) = g_0(X) + h(T)$ with $h \in k[T]$ additive hence a p-polynomial, thus we conclude by applying to h the case $n = 1$. Let us fix $x \in k^n$. Then by additivity $f(x, T) + f(0, 0) = f(x, 0) + f(0, T) \in k[T]$. By developing both terms, we get

$$g_1(x)T + \ldots + g_m(x)T^m = g_1(0)T + \ldots + g_m(0)T^m \in k[T],$$

hence $g_i(x) = g_i(0)$ is constant for all i.

□

Definition 4.1.5. A nonzero polynomial $f \in k[X_1, \ldots, X_n]$ is a **separable** polynomial if $A := k[X_1, \ldots, X_n]/(f)$ is a separable k-algebra, that is, geometrically reduced.

Proposition 4.1.6. *Let $f \in k[X_1, \ldots, X_n]$ be a nonzero polynomial such that $f(0) = 0$. Then the subscheme $f^{-1}(0) \subseteq \mathbb{G}_a^n$ is a smooth k-subgroup of $\mathbb{G}_a^n$ if and only if f is a separable p-polynomial.*

Proof. Let f be a p-polynomial: the subscheme $f^{-1}(0)$ is the kernel of the associated map $\mathbb{G}_a^n \to \mathbb{G}_a$, which is a k-homomorphism by 4.1.4, hence $f^{-1}(0)$ is a k-subgroup. By definition of separable polynomial, it is also generically smooth, thus being a k-group, it is smooth.
Conversely, let $G := f^{-1}(0) \subseteq \mathbb{G}_a^n$ be a smooth k-subgroup. The smoothness implies by definition that f is separable. Again by 4.1.4, it suffices to prove that the associated map of schemes is a k-homomorphism, i.e. that f is additive. Since it suffices to verify this after extending scalars to $\bar{k}$, and smoothness being a geometric property, we can suppose that k is algebraically closed. Let $\alpha \in G(k)$: since $G \subseteq \mathbb{G}_a^n$ is a k-subgroup, $x + \alpha$ belongs to G if and only if x does, thus $f(X + \alpha)$ and $f(X)$ both have G as zero scheme in affine space. Hence there exists a unique constant $\lambda(\alpha) \in k^\times$ such that $f(X + \alpha) = \lambda(\alpha) f(X)$. By considering a monomial of highest degree of f we obtain $\lambda(\alpha) = 1$. Now let us fix $\beta \in k^n$. Since $f(\alpha + \beta) = f(\beta)$ for all $\alpha \in G(k)$, the polynomial $f(X + \beta) - f(X)$ vanishes on $G(k)$. The group G being smooth and k algebraically closed, G is the only reduced subscheme of $\mathbb{G}_a^n$ having as underlying topological space the Zariski closure of $G(k)$, which allows to conclude that $f(X + \beta) - f(\beta)$ vanishes on all G. Therefore there exists a unique $\mu(\beta) \in k$ such that $f(X + \beta) - f(\beta) = \mu(\beta) f(X)$. Considering a monomial term of highest degree we obtain $\mu(\beta) = 1$, hence $f(x + \beta) = f(x) + f(\beta)$ for all x, $\beta \in k^n$ and f is additive. □

Corollary 4.1.7. *Let $G \subseteq \mathbb{G}_a^n$ be a smooth k-subgroup of codimension 1. Then G is the zero scheme of a separable nonzero polynomial in $k[X_1, \dots, X_n]$.*

Proof. Being a smooth closed subscheme of codimension 1, G is the zero scheme of a separable nonzero polynomial $f \in k[X_1, \dots, X_n]$. By 4.1.4, the fact that $G = f^{-1}(0)$ is a k-subgroup implies that f is a p-polynomial. □

Definition 4.1.8. Let $f = \sum_{i=1}^n f_i(X_i)$ be a p-polynomial over k in n variables with $f_i(0) = 0$ for all i. The **principal part** of f is the sum of the leading terms of the f_i.

Lemma 4.1.9. *Let V be a vector group of dimension $n \geqslant 1$ over k and let $f\colon V \to \mathbb{G}_a$ be a k-homomorphism. The following are equivalent.*

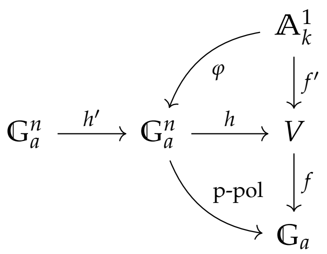
1. *There exists a nonconstant k-scheme morphism $f'\colon \mathbb{A}_k^1 \to V$ such that $f \circ f' = 0$.*
2. *For every k-group isomorphism $h\colon \mathbb{G}_a^n \simeq V$, the principal part of the nonzero p-polynomial $f \circ h$ has a nontrivial zero in k^n.*
3. *There exists a k-group isomorphism $h\colon \mathbb{G}_a^n \simeq V$ such that $\ker(f \circ h)$ contains the first factor of $\mathbb{G}_a^n$, i.e. $f \circ h$ only depends on the last $n-1$ coordinates.*

Remark 4.1.10. In the second condition, the existence of such an isomorphism is not sufficient: let k be imperfect and consider $a \in k \backslash k^p$, $f(X,Y) = Y^p - (X + aX^p)$. Then f is a nonzero p-polynomial whose principal part $Y^p - aX^p$ has no zeros on $k^2 \backslash \{0\}$. However, by composing it with the k-automorphism of $\mathbb{G}_a^2$ given by $h\colon (x,y) \mapsto (x, y + x^p)$ one gets the p-polynomial $f \circ h = Y^p + X^{p^2} - (X + aX^p)$, whose principal part is $Y^p + X^{p^2}$ which has $(1,-1)$ as nontrivial zero.

Proof. (1) ⇒ (2) : Let $\varphi := h^{-1} \circ f'$ and write it in components as $\varphi = (\varphi_1, \dots, \varphi_n)$, with $\varphi_i \in k[t]$. Let $s_i = 0$ whenever $\varphi_i = 0$ and denote $a_i t^{s_i}$ the leading term of φ_i otherwise. Since f' is not constant, the same holds for φ, hence for some i we have $s_i > 0$. Let $f = \sum_{i=1}^n c_i X_i^{p^{m_i}}$ be the principal part of $f \circ h$. By (1), $0 = f \circ f' = (f \circ h) \circ (h^{-1} \circ f') = f \circ h \circ \varphi$, hence

$$0 = f(h(\varphi(t))) = \sum_{i=1}^n c_i (a_i t^{s_i})^{p^{m_i}} + \dots = \sum_{i=1}^n c_i a_i^{p^{m_i}} t^{s_i p^{m_i}} + \dots$$

Now let $N := \max_i \{s_i p^{m_i}\} > 0$ and define $b_i := a_i$ when $s_i p^{m_i} = N$ (so in particular b_i is nonzero) and $b_i := 0$ otherwise. The coefficient of the term of degree N in $f \circ h \circ \varphi$ is $\sum_{i=1}^n c_i b_i^{p^{m_i}}$ and it must vanish, hence $(b_1, \dots, b_n)$ is the desired nontrivial zero of the principal part of $f \circ h$.



(2) ⇒ (3) : Let $h\colon \mathbb{G}_a^n \simeq V$ be a k-group isomorphism. The case $f = 0$ is trivial, hence we may assume $f \neq 0$ so the principal part of $f \circ h$ is nonzero: we denote it as $\sum_{i=1}^n c_i X_i^{p^{m_i}}$. Let d be the sum of the degrees of its nonzero terms and let us proceed by induction on d, the case $d = 0$ being

$f = 0$. If $c_r = 0$ for some r, the principal part does not depend on X_r, hence the same holds for the whole p-polynomial $f \circ h$, so we are done by composing with the k-automorphism interchanging X_1 and X_r. Thus, let us assume that all c_i are nonzero and, up to a coordinate permutation, that $m_1 \geqslant \ldots \geqslant m_n \geqslant 0$. By (2), there exists $(a_1, \ldots, a_n) \in k^n \backslash \{0\}$ such that $\sum_{i=1}^n c_i a_i^{p^{m_i}} = 0$. Let $r \geqslant 0$ be minimal such that $a_r \neq 0$ and define the k-automorphism $h' \colon \mathbb{G}_a^n \simeq \mathbb{G}_a^n$ given by

$$(y_1, \ldots, y_n) \longmapsto (x_1, \ldots, x_n) := (y_1, \ldots, y_{r-1}, a_r y_r, y_{r+1} + a_{r+1} y_r^{p^{m_r - m_{r+1}}}, \ldots, y_n + a_n y_r^{p^{m_r - m_n}})$$

By composing the principal part of $f \circ h$ with h' we get

$$\sum_{i=1}^{n} c_i X_i^{p^{m_i}} = \sum_{i=1}^{r-1} c_i Y_i^{p^{m_i}} + c_r a_r^{p^{m_i}} Y_r^{p^{m_i}} + \sum_{i=r+1}^{n} c_i \left(Y_i + a_i Y_r^{p^{m_r - m_i}} \right)^{p^{m_i}} = \sum_{i \neq r} c_i Y_i^{p^{m_i}} + \sum_{i=r}^{n} c_i a_i^{p^{m_i}} Y_r^{p^{m_r}}$$

which since $a_1 = \ldots = a_{r-1} = 0$, equals

$$\sum_{i \neq r} c_i Y_i^{p^{m_i}} + \left(\sum_{i=1}^{n} c_i a_i^{p^{m_i}} \right) Y_r^{p^{m_r}} = \sum_{i \neq r} c_i Y_i^{p^{m_i}}$$

because $(a_1, \ldots, a_n)$ is a zero. Finally, the sum of the degrees of the nonzero terms of the principal part of $f \circ h \circ h'$ is strictly smaller than d (because $c_r \neq 0$) and we conclude by applying the induction hypothesis.
(3) $\Rightarrow$ (1) : Let $h \colon \mathbb{G}_a^n \to V$ be a k-group isomorphism such that $\ker(f \circ h)$ contains the first factor of $\mathbb{G}_a^n$. Define $\varphi \colon \mathbb{G}_a \to \mathbb{G}_a^n$ as $\varphi(t) = (t, 0, \ldots, 0)$ and let $f' := h \circ \varphi$. Then $f(f'(t)) = f(h(\varphi(t))) = f(h(t, 0, \ldots, 0))$ hence $f \circ f' = 0$. □

Lemma 4.1.11. *Let V be a vector group of dimension $n \geqslant 1$ over k, K/k a Galois extension, and let $f \colon V \to \mathbb{G}_a^n$ be a k-homomorphism. The equivalent conditions of 4.1.9 hold over K if and only if they hold over k.*

Proof. First, we prove the following : if f is a p-polynomial of the form $f(X) = \sum_{i=1}^n c_i X_i^{p^{m_i}}$ over k, then if f has a zero in $K^n \backslash \{0\}$, then it has a zero in $k^n \backslash \{0\}$.
We proceed by induction on n: if $n = 1$, by hypothesis there exists $a_1 \in K^\times$ such that $c_1 a_1^{p^{m_1}} = 0$, then $c_1 = 0$ and we conclude. If $n > 1$, we can suppose up to permuting the coordinates that $m_1 \geqslant \ldots \geqslant m_n$ and consider $(a_1, \ldots, a_n) \in K^n \backslash \{0\}$ such that $\sum_{i=1}^n c_i a_i^{p^{m_i}} = 0$. If $a_n = 0$, then we can apply the induction hypothesis to $\sum_{i=1}^{n-1} c_i X_i^{p^{m_i}}$. Otherwise, we can divide each a_i by $a_n^{p^{m_n - m_i}}$ and thus assume that $a_n = 1$. Now let $\sigma \in Gal(K/k)$: both a and $\sigma(a)$ are zeros of f, and since it is a p-polynomial, $b := a - \sigma(a)$ is a zero too. If all a_i belong to k already, we are done; if not, since the extension is Galois, there exists a σ such that $a \neq \sigma(a)$ hence $b \neq 0$. Moreover, $b_n = a_n - \sigma(a_n) = 1 - 1 = 0$, so we can again apply the induction hypothesis.
Now let us go back to the conditions in 4.1.9. If (1) is true over k, then it is also true over K. Moreover, we just proved that if the principal part of a nonzero p-polynomial has a nontrivial zero in K^n, then it has a nontrivial zero in k^n, which means that if (2) holds over K, then it also holds over k. □

4.1.2 Embedding into a vector group and consequences

Theorem 4.1.12. *Let G be a smooth p-torsion commutative k-group. Then*

(a) G embeds as a k-subgroup of a vector group over k,

(b) *G admits an* ***étale isogeny*** *onto a vector group over* k,

(c) *If* G *is connected and* $k = \overline{k}$, *then* G *is a vector group over* k.

Let us recall some notations and basic facts on the Lie algebra of a vector group, which we will need in the proof : for any finite dimensional k-vector space V, the associated vector group $\underline{V} \simeq \mathrm{Spec}(Sym(V^\vee))$ represents the functor $(\mathrm{k}-\mathbf{Alg}) \to (\mathbf{Grp})$, $R \mapsto V \otimes R$. A choice of a basis for V determines an isomorphism $\underline{V} \simeq \mathbb{G}_a^n$ for some integer n. Let $W = \underline{V}$ be a vector group. Then

$$\mathcal{O}(W) = \mathcal{O}(\underline{V}) = Sym(V^\vee) = \bigoplus_{n \geqslant 0} (V^\vee)^{\otimes n} / \langle v \otimes w - w \otimes v \mid v, w \in V^\vee \rangle$$

has augmentation ideal $I = \ker \epsilon = \bigoplus_{n \geqslant 1} (V^\vee)^{\otimes n}$, hence $I/I^2 = (V^\vee)^{\otimes 1} = V^\vee$ and

$$\mathrm{Lie}(W) \simeq \mathrm{Hom}_k(I/I^2, k) = \mathrm{Hom}_k(V^\vee, k) \simeq V,$$

so $W = \underline{V} \simeq \underline{\mathrm{Lie}(W)}$.

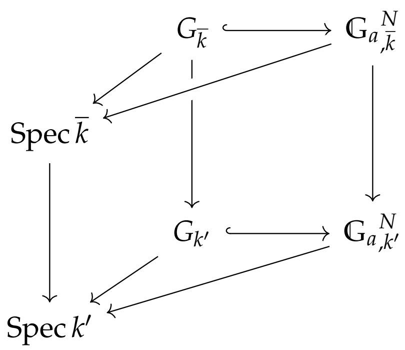
Proof. (a) : Let us start by constructing the embedding into a vector group over k. First, we want to show that we can assume $k = \overline{k}$.
Let k'/k be a finite extension and consider the canonical inclusion $i_G \colon G \hookrightarrow \mathcal{R}_{k'/k}(G_{k'})$ defined in Proposition 3.1.3. By definition of Weil restriction,

$$\mathcal{R}_{k'/k}(\mathbb{G}_{a,k'})(R) = \mathbb{G}_{a,k'}(R \otimes k') = R \otimes k' \simeq R^{[k' : k]},$$

for all k-algebras R, i.e. $\mathcal{R}_{k'/k}(\mathbb{G}_{a,k'}) \simeq \mathbb{G}_a^{[k' : k]}$. Now if $G_{k'}$ embeds as a k'-subgroup of $\mathbb{G}_{a,k'}^n$, by applying the functor $\mathcal{R}_{k'/k}$, which is right adjoint to base change hence left exact hence preserves kernels, we get

$$G \hookrightarrow \mathcal{R}_{k'/k}(G_{k'}) \hookrightarrow \mathcal{R}_{k'/k}(\mathbb{G}_{a,k'}^n) = \mathbb{G}_a^{n \cdot [k' : k]}$$

This allows us to replace k with a finite extension k'. Now suppose there exists an embedding of $G_{\overline{k}}$ as a $\overline{k}$-subgroup of some $\mathbb{G}_{a,\overline{k}}^N$. Using standard arguments on limits of schemes, since $\overline{k}$ is the direct limit of its finite subextensions $k \subset k' \subset \overline{k}$, the embedding descends to a finite extension k', i.e. there exists k' such that the following diagram commutes.



Therefore we can assume that k is algebraically closed.
Next, we want to prove that we can assume G is connected. For this, let us consider the component group G/G^o. It is étale, hence since $k = \overline{k}$ it must be a constant discrete commutative group. Moreover,

G is p-torsion hence it must be the constant group over k associated to the abstract group $(\mathbb{Z}/p\mathbb{Z})^n$ for some n. Now let us consider the connected-étale sequence on rational points:

$$1 \longrightarrow G^o(k) \longrightarrow G(k) \longrightarrow (\mathbb{Z}/p\mathbb{Z})^n\,(k) \longrightarrow 1.$$

Let us fix $\overline{x_1}, \dots, \overline{x_n}$ a $(\mathbb{Z}/p\mathbb{Z})$- basis of $G/G^o(k)$: then any choice of liftings $x_1, \dots, x_n$ in $G(k)$ generates a subgroup isomorphic to $(\mathbb{Z}/p\mathbb{Z})^n$ because G is p-torsion. This splits the sequence over k-points, which actually gives a splitting of algebraic groups, because $(\mathbb{Z}/p\mathbb{Z})^n$ is a constant group hence a sum of k-points. Thus there exists an isomorphism $G \simeq G^o \times (\mathbb{Z}/p\mathbb{Z})^n$, and since $(\mathbb{Z}/p\mathbb{Z})$ is a k-subgroup of the additive group, G embeds into $G^o \times \mathbb{G}_a^n$. Therefore we can conclude that, for the purpose of finding an embedding of G into a vector group, we can assume that G is connected.
Our aim is actually to prove that, under these two assumptions, G is a vector group. By Corollary 1.2.6, G being connected and unipotent over $\overline{k}$, it admits a composition series with successive quotients isomorphic to $\mathbb{G}_a$, which we denote as $G = G_0 \supset G_1 \supset \cdots \supset G_s = 1$. In particular each G_i is a commutative extension of $\mathbb{G}_a$ by G_{i+1}. By induction on the dimension of G, it suffices to prove that a commutative extension U of $\mathbb{G}_a$ by $\mathbb{G}_a$ is k-split if it's p-torsion.
For this, consider the group $W_{2,k}$ of Witt vectors of order 2 and the canonical short exact sequence

$$0 \longrightarrow \mathbb{G}_a \xrightarrow{\mathcal{I}_n} W_{2,k} \xrightarrow{\pi_{1,1}} \mathbb{G}_a \longrightarrow 1.$$

By Proposition 2.2.12, the element $\mathcal{E}_1 \in \operatorname{Ext}^1(\mathbb{G}_a, \mathbb{G}_a)$ corresponding to the isomorphism class of this extension is a basis of the left $k[\mathbf{F}]$-module $\operatorname{Ext}^1(\mathbb{G}_a, \mathbb{G}_a)$. In other words, there exists a k-group endomorphism φ of the additive group such that U is given by the following cartesian diagram:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathbb{G}_a & \longrightarrow & & \xrightarrow{q} & \mathbb{G}_a & \longrightarrow & 1 \\
 & & \| & & \downarrow{\scriptstyle\psi} & & \downarrow{\scriptstyle\varphi} & & \\
1 & \longrightarrow & \mathbb{G}_a & \longrightarrow & W_{2,k} & \xrightarrow{\pi_{1,1}} & \mathbb{G}_a & \longrightarrow & 1.
\end{array}$$

Since U is smooth and p-torsion, the same is true for the subgroup $\psi(U)$. Moreover,

$$p \cdot (x, y) = (0, x^p) \qquad \text{for all } (x, y) \in W_{2,k},$$

hence in particular, if we denote H the p-torsion subgroup of $W_{2,k}$, we have $\pi_{1,1}(H) = \alpha_p$. It follows that $\pi_{1,1} \circ \psi(U)$ is a smooth subgroup of α_p hence it is trivial. By commutativity of the pullback diagram above, $\pi_{1,1} \circ \psi = \varphi \circ q$ vanishes hence $\varphi = 0$ because q is an epimorphism. Thus, we conclude that the extension must be split i.e. $U \simeq \mathbb{G}_a^2$.
Having proved (a) and (c), we can go back to the general setting of an arbitrary base field k in order to construct the étale isogeny. Let us fix an embedding of G into a vector group V, having codimension m. Consider the vector subspace $\operatorname{Lie}(G) \subseteq \operatorname{Lie}(V)$: once we have fixed an isomorphism $V \simeq \mathbb{G}_a^n$ for some n, the map $W \mapsto \operatorname{Lie}(W)$ gives a bijection between linear k-subgroups of V and vector subspaces of $\operatorname{Lie}(V)$, so we can choose such a W such that $\operatorname{Lie}(G) \oplus \operatorname{Lie}(W) = \operatorname{Lie}(V)$ and consider the map $\rho\colon G \hookrightarrow V \twoheadrightarrow V/W$. The associated linear map

$$\operatorname{Lie}\rho\colon \operatorname{Lie}(G) \to \operatorname{Lie}(V/W)$$

is an isomorphism of Lie algebras. Let $N := \ker \rho$: since G is smooth and connected, the equality $0 = \ker(\mathrm{Lie}\,\rho) = \mathrm{Lie}(\ker \rho) = \mathrm{Lie}\, N$ implies that N is smooth of dimension 0, hence étale. The closed immersion $G/N \hookrightarrow V/W$ given by universal property of the quotient must hence be also an open immersion, so it is an isomorphism because the vector group V/W is connected. In conclusion, ρ is surjective with finite étale kernel, hence it is the desired étale isogeny of G into a vector group. □

We will now state and prove some consequences of the embedding of a smooth p-torsion commutative group into a vector group. In particular, the following result will be useful later, when we will need to consider k-scheme morphism from the affine line.

Proposition 4.1.13. *Let $V_1, \ldots, V_n$ be k-groups isomorphic to $\mathbb{G}_a$ and let $V := V_1 \times \cdots \times V_n \simeq \mathbb{G}_a^n$. Let U be a smooth k-subgroup of V such that U_{k_s} is the k_s-subgroup of V_{k_s} generated by a family of k_s-scheme morphisms $\varphi \colon \mathbb{A}^1_{k_s} \to V_{k_s}$ passing through 0. There exists a k-group automorphism h of V such that $h(U)$ is the direct product $V_1 \times \cdots \times V_r$ for some $r \leqslant n$. In particular this shows that*

*(i) U is a **vector group** over k,*

*(ii) U is a k-group **direct factor** of V.*

Proof. Let us proceed by induction on n. If $n = 1$, it suffices to take the identity morphism $\mathbb{A}^1_{k_s} \to V_{1,k_s}$ to conclude that $U_{k_s} = V_{1,k_s}$ and so $U = V_1$. Now let $n > 1$. If $\dim U = \dim V = n$, then being smooth and connected we conclude that $U = V$, so we can suppose $\dim U \leqslant n-1$. If $\dim U = n-1$, then by 4.1.15 U is the zero scheme of a p-polynomial, i.e. the kernel of some homomorphism $f \colon V \to \mathbb{G}_a$. Since we assumed that U has dimension $n-1 > 0$, there exists a nonconstant scheme morphism $f' \colon \mathbb{A}^1_{k_s} \to V_{k_s}$ such that $U_{k_s} = f^{-1}(0)_{k_s}$ contains the image of f'. In particular, $f' \circ f = 0$ over k_s : by applying Lemma 4.1.11 to the extension k_s/k and the equivalence (1) ⇔ (3) in Lemma 4.1.9, we conclude the existence of a k-group automorphism $h' \colon V \xrightarrow{\sim} V$ such that $\ker(f \circ h')$ contains V_1. The group U being the zero scheme of f, this is equivalent to saying that V_1 is contained in $h'(U)$. Let us denote as U' the projection of $h'(U)$ onto $V' := V_2 \times \cdots \times V_n$, then we have $h'(U) = V_1 \times U'$, so we can apply the induction hypothesis to U' and V' to conclude. Finally, let us suppose that $\dim U$ is strictly smaller than $n-1$ and let U' be the projection of U onto $V' = V_2 \times \cdots \times V_n$. By the inductive hypothesis, there exists a k-group automorphism $h \colon V' \xrightarrow{\sim} V'$ such that $h(U') = V_2 \times \cdots \times V_r$ for some $r < n$. If we set $h' := \mathrm{id}_{V_1} \times h \colon V \simeq V$, we obtain $h'(U) \subseteq V_1 \times \cdots \times V_r$ and we can again apply induction as before. □

Corollary 4.1.14. *Let G be a smooth p-torsion commutative k-group. Then any smooth k-subgroup of G which is a vector group is a k-group direct factor.*

Proof. By 4.1.12, the group G embeds as a k-subgroup of some vector group V of dimension n over k. Let us consider a smooth k-subgroup W which is isomorphic to $\mathbb{G}_a^r$ for some $r \leqslant n$. The vector group W is generated by k-homomorphisms

$$\mathbb{G}_a \hookrightarrow \mathbb{G}_a^r \xrightarrow{\sim} W \hookrightarrow G \hookrightarrow V,$$

hence in particular by k-scheme morphisms $\mathbb{A}^1_k \to V$, so we can apply Proposition 4.1.13 to conclude that W is a k-group direct factor inside of V, hence in particular by restriction a direct factor of G. □

Another important consequence of Theorem 4.1.12 is the following : in the case of an infinite base field, we can actually find an embedding into a vector group having codimension equal to 1.

Proposition 4.1.15. *Let U be a smooth p-torsion commutative k-group over an infinite field k. Then U is isomorphic to a k-subgroup of* ***codimension 1*** *of a k-vector group. In particular, it is isomorphic to the zero scheme of a separable nonzero p-polynomial over k.*

Later we will see that if k is perfect and U is connected then it is a vector group (see Corollary 4.2.5 below) : this proposition is thus true also over finite fields if U is connected.

Example 4.1.16. Actually, this result is not tautological : in the case of a finite base field k, a nonconnected U with the properties above does not admit an embedding of codimension 1 in general. Let $k = \mathbb{F}_p$: then $\mathbb{G}_{a,k}$ consists of p rational points. Hence, for $n > 1$ the constant group $U := (\mathbb{Z}/p\mathbb{Z})^n$ has dimension 0 but it cannot admit an embedding into the additive group because it is a disjoint sum of p^n rational points.

Proof. By Theorem 4.1.12, there exists an embedding of G into a vector group V over k. Let us proceed by induction on $m := \dim V - \dim U$. If $m = 1$, then we conclude using Corollary 4.1.7. Let us assume $m > 1$: if we prove that U can be embedded into a vector group W over k of dimension equal to $\dim V - 1$, then we are done by induction. By smoothness of U, the linear subspace $\mathrm{Lie}(U)$ has codimension m in $\mathrm{Lie}(V)$. Let us fix an isomorphism $V \simeq \mathbb{G}_a^n$, with its corresponding linear structure on V, and consider the schematic image of the multiplication map $\mathbb{G}_a \times U \to V$, which we denote as Y. Since $m \geqslant 2$, the closed subscheme Y has nonzero codimension in V. Now let us consider the vector group $\underline{\mathrm{Lie}(U)} \subseteq V$ associated to the linear subspace $\mathrm{Lie}(U)$: since V is irreducible, the union $\underline{\mathrm{Lie}(U)} \cup Y$ must be a proper closed subscheme of V. Moreover, k is infinite and the underlying scheme of V is the affine space $\mathbb{A}_k^n$, so the set of rational points $V(k)$ is dense in V. Thus, let us take v a rational point not belonging to $\underline{\mathrm{Lie}(U)} \cup Y$ and denote $L \subset V$ the k-subgroup corresponding to the line $\langle v \rangle \subset V(k)$. Consider $\pi\colon V \twoheadrightarrow W := V/L$ the canonical quotient map and set $\psi := \pi_{|U}$: it is enough to prove that $\ker \psi = 1$, so U embeds as a k-subgroup of W. For this, let us consider the induced Lie algebra homomorphism

$$\mathrm{Lie}\,\psi\colon\ \mathrm{Lie}(U) \longrightarrow \mathrm{Lie}(W) = \mathrm{Lie}(V)/\mathrm{Lie}(L).$$

Its kernel is given by $L \cap \underline{\mathrm{Lie}(U)}$, which is trivial because $v \notin \mathrm{Lie}(U)$. Hence we obtain $0 = \ker(\mathrm{Lie}\,\psi) = \mathrm{Lie}(\ker \psi)$. Since the group U is smooth and connected, $\ker \psi$ is étale, i.e. of the form $\mathrm{Spec}\,A$ with A a finite étale k-algebra. By extending scalars to an algebraic closure, $(\ker \psi)_{\overline{k}} = \mathrm{Spec}(A \otimes \overline{k})$ is a disjoint union of n copies of $\mathrm{Spec}\,\overline{k}$, where n denotes the dimension of A as a k-vector space. Thus, it suffices to prove that ψ is injective on $U(\overline{k})$: if this holds, then $n = 1$ hence $A = k$ and $\ker \psi$ is trivial. Now, if ψ is not injective on $U(\overline{k})$, then there exists a nonzero $\lambda \in k$ such that $\lambda v \in U(\overline{k})$. Since Y is stable under the action $\mathbb{G}_a \times V \to V$, this would imply $\langle v \rangle = L(k) \subseteq Y(k)$. However, by definition v belongs to $L(k)$ but not to Y, so we conclude that $\psi_{U(\overline{k})}$ is injective. ☐

4.2 Wound unipotent groups

Let us recall that a torus over k is k-anisotropic, i.e. $X(T) = \mathrm{Hom}_{(\mathrm{k-\mathbf{Grp}})}(T, \mathbb{G}_m) = 1$, if and only if $\mathrm{Hom}_{(\mathrm{k-\mathbf{Grp}})}(\mathbb{G}_m, T) = 1$: if we consider a nontrivial character $\chi\colon T \to \mathbb{G}_m$, the image $\chi(T)$ is a smooth connected nontrivial k-subgroup of $\mathbb{G}_m$, hence it coincides with $\mathbb{G}_m$. By setting $T' := \ker \chi$, the following sequence is exact

$$1 \longrightarrow T' \longrightarrow T \longrightarrow \mathbb{G}_m \longrightarrow 1.$$

Since T' is of multiplicative type, this is an exact sequence in the semisimple abelian category of groups of multiplicative type, hence there is a splitting $T \simeq T' \times \mathbb{G}_m$. This gives a nontrivial isomorphism $f\colon \mathbb{G}_m \to T = T' \times \mathbb{G}_m$, $x \mapsto (1, x)$.
For unipotent groups, the analogous statement obtained by remplacing $\mathbb{G}_m$ by $\mathbb{G}_a$ fails : by Proposition 1.2.7, every unipotent k-group admits nontrivial k-homomorphisms to $\mathbb{G}_a$, however the group U defined in 4.1.2 does not contain $\mathbb{G}_a$ as a k-subgroup.
Taking these considerations into account, it is natural to consider as the analogous to k-anisotropicity the property of admitting no nontrivial homomorphisms from $\mathbb{G}_a$. However, it is more convenient to give another definition by considering maps of schemes from the affine line, and later prove that the two coincide.

Definition 4.2.1. A smooth connected unipotent k-group U is ***k*-wound** if every k-scheme morphism $\mathbb{A}^1_k \to U$ is a constant map to a point in $U(k)$.

Example 4.2.2. The following examples show that over an imperfect field the k-wound property behaves in a very unusual way.

- If a torus is k-anisotropic, then it stays anisotropic after a purely inseparable extension of the base field, while the k-wound property can be lost under such an extension : let k be imperfect and $t \in k \backslash k^p$. By 4.1.2, the k-subgroup $U = \{y^p = x - tx^p\}$ of $\mathbb{G}_a^2$ becomes isomorphic to $\mathbb{G}_{ak'}$ over $k' = k(t^{1/p})$. However, it does not admit any nonconstant k-scheme morphism from the affine line: let $\varphi\colon \mathbb{A}^1_k \to U$ be such a map, then the image $\varphi(\mathbb{A}^1_k)$ is connected and is not just a point. So, since U is irreducible, φ is a dominant morphism. Hence it extends to a finite surjective map $\overline{\varphi}\colon \mathbb{P}^1_k \to \widetilde{U}$ where $\widetilde{U}$ denotes the regular compactification of U. This gives a contradiction because $\overline{\varphi}$ must send the unique point at infinity of $\mathbb{A}^1_k$, which is k-rational, to the point at infinity of $\widetilde{U}$, which is not k-rational.

- A smooth connected subgroup of a k-split torus is still k-split, while a k-split unipotent group can admit nontrivial k-wound subgroups : the group U is a k-wound subgroup of $\mathbb{G}_a^2$.

- A nontrivial quotient of a k-wound group by a k-wound subgroup can be k-split : let k be imperfect and $t \in k \backslash k^p$. The k-subgroup of $\mathbb{G}_a^3$ given by

$$G(R) := \{(x, y, z) \in R^3\colon x^{p^2} + t^p y^{p^2} + tz^p = x\} \subseteq R^3,$$

for all k-algebras R, is the zero scheme in affine space of the separable p-polynomial $X^{p^2} + t^p Y^{p^2} + tZ^p - X$, whose principal part $X^{p^2} + t^p Y^{p^2} + tZ^p$ has no nontrivial zero on k^3. Assume there exists a nonconstant k-scheme morphism $\varphi\colon \mathbb{A}^1_k \to G$. Composing with the inclusion of G in $\mathbb{G}_a^3$ gives a nonconstant k-scheme morphism $f'\colon \mathbb{A}^1_k \to \mathbb{G}_a^3$ such that $f \circ f' = 0$. By 4.1.9, taking as h the identity of $\mathbb{G}_a^3$ gives a contradiction. Hence G is k-wound. Moreover, its subgroup $H = \{(x, y, z) \in G\colon z = 0\}$ is smooth, connected and k-wound, and the map

$$G \longrightarrow \mathbb{G}_a, \quad (x, y, z) \longmapsto z$$

induces an isomorphism of k-groups $G/H \simeq \mathbb{G}_a$. This example is from [Oes84, Ch V, 3.5].

This last example shows that there is a link between p-polynomials and k-wound groups: let us illustrate it in detail in the case of an infinite field k. By Proposition 4.1.15, smooth p-torsion commutative k-groups are of the form $U = f^{-1}(0) \subseteq \mathbb{G}_a^n$ with f a separable p-polynomial. Moreover, algebraic groups are connected if and only if they are geometrically irreducible, hence such a U is connected if and only if f is geometrically irreducible over k. Let us suppose U is connected : if its principal part has no nontrivial zero in k^n, then by applying Lemma 4.1.9 as in the example above we get that U is k-wound, but the converse is false (see Remark 4.1.10). However assume there exists a nontrivial k-rational zero: following the proof of (2) $\Rightarrow$ (3) in 4.1.9 and setting $h = \mathrm{id}_{\mathbb{G}_a^n}$, we obtain that U is isomorphic as a k-group to $F^{-1}(0)$, where F is a nonzero p-polynomial which is still geometrically irreducible over k, but the sum of the degrees of the monomials of its principal part is strictly smaller than the one for f. By repeating this argument, one eventually gets a principal part having no nontrivial zero in k^n. So all smooth p-torsion commmutative k-wound groups can be realized as zero schemes of geometrically irreducible p-polynomials whose principal part has no nontrivial k-rational zero.

The following result gives a canonical decomposition of smooth connected p-torsion commutative k-groups using the notions that we just introduced.

Theorem 4.2.3. *Let U be a smooth connected p-torsion commutative k-group. Then it is a direct product*

$$U = V \times W$$

of a vector group V over k and a smooth connected unipotent k-group W such that W_{k_s} is k_s-wound. The subgroup V is uniquely determined by the following : V_{k_s} is generated by all k_s-scheme morphisms $\varphi\colon \mathbb{A}^1_{k_s} \to U_{k_s}$ passing through 0.

Proof. Let us consider the unique smooth connected k_s-subgroup $\widetilde{V}$ of U_{k_s} which is generated by all k_s-scheme morphisms $\varphi\colon \mathbb{A}^1_{k_s} \to U_{k_s}$ passing through 0. Since k_s/k is a Galois extension, by Galois descent there exists a unique k-subgroup V of U such that $V_{k_s} = \widetilde{V}$, which is necessarily smooth and connected. By 4.1.12, the group U admits an embedding into $\mathbb{G}_a^N$ for some $N \geqslant 1$, hence the same is true for V. Applying 4.1.13 and 4.1.14 to V, we get that V is a vector group over k and in particular a k-group direct factor of U. Hence there exists a k-subgroup W of U and a splitting $U = V \times W$. By hypothesis U is smooth, connected and unipotent, so the same holds for W. Moreover, W_{k_s} is a k_s-wound subgroup due the definition of $\widetilde{V}$, so it remains to show that V is unique. For this, let us consider a second decomposition $U = V' \times W'$ with V' a vector group over k and W' a smooth connected unipotent k-subgroup of U such that W'_{k_s} is k_s-wound. If $\varphi\colon \mathbb{A}^1_{k_s} \to U_{k_s}$ is a k_s-scheme morphism, then by composing with the projection $U_{k_s} \twoheadrightarrow W'_{k_s}$ we obtain a k_s-scheme morphism from the affine line to W'_{k_s} which must be constant by definition of k_s-wound. Therefore, if φ passes through 0, then its image is contained in V'_{k_s} : this proves the inclusion $V \subseteq V'$. Both are vector groups, hence $V' = V \times V''$, where V'' denotes the image of V' under the projection $U \twoheadrightarrow W$. In particular, V''_{k_s} is a vector group over k_s and a subgroup of W_{k_s}. Since the latter is k_s-wound, such a subgroup is trivial, hence $V'' = 0$ and finally $V = V'$. □

Corollary 4.2.4. *The following are equivalent for a smooth connected p-torsion commutative k-group U:*

(a) U is k-wound,

(b) U_{k_s} is k_s-wound,

(c) every k-homomorphism $\mathbb{G}_a \to U$ is trivial.

Moreover, U is a vector group over k if and only if U_{k_s} is a vector group over k_s.

Proof. $(a) \Rightarrow (c)$: a nontrivial k-homomorphism $\mathbb{G}_a \to U$ is in particular a nontrivial k-scheme morphism $\mathbb{A}^1_k \to U$.
$(c) \Rightarrow (b)$: assume U_{k_s} is not k_s-wound. Keeping the same notations as in the above theorem, this implies that $V_{k_s} \neq 0$. This implies that $V \neq 0$ too, so since V is a nontrivial vector group over k, there exists a nontrivial morphism $\mathbb{G}_a \hookrightarrow V$.
$(b) \Rightarrow (a)$: let U_{k_s} be k_s-wound and consider the decomposition $U = V \times W$ given by the theorem. Since $U_{k_s} = V_{k_s} \times W_{k_s}$ with V_{k_s} a vector group over k_s, we must have $V_{k_s} = 0$ hence there are no nontrivial k_s-scheme morphisms $\varphi\colon \mathbb{A}^1_{k_s} \to U_{k_s}$ passing through 0. If we had a nonconstant map of k-schemes $\mathbb{A}^1_k \to U$, by a translation and by extending scalars to k_s we would obtain such a φ, hence U is k-wound.
Finally, let U_{k_s} be a vector group over k_s: then $U_{k_s} = V_{k_s}$ hence $W_{k_s} = 0$, which implies $W = 0$ and $U = V$ is a vector group over k. □

Corollary 4.2.5. *If k is a perfect field, a smooth connected p-torsion commutative k-group is a vector group.*

Proof. Since $k_s = \overline{k}$, we can suppose that k is algebraically closed and apply Theorem 4.1.12. □

Let us give an example of a k-wound subgroup arising as the quotient of a pseudo-reductive commutative group.

Let G be a commutative pseudo-reductive group over k. By [SGA3, XII, Theorem 1.7], all tori of maximal dimension are conjugated in G by a k'-rational point for some finite separable extension k'/k. The group G being commutative, this implies that there exists a unique maximal k-torus $T \subset G$. By the structure theorem of commutative affine algebraic groups ([SGA3, $XVII$, Theorem 7.2.1]) applied to the smooth and connected G, the quotient $U := G/T$ is a smooth connected commutative unipotent k-group.

Lemma 4.2.6. *With the above notations, the quotient*

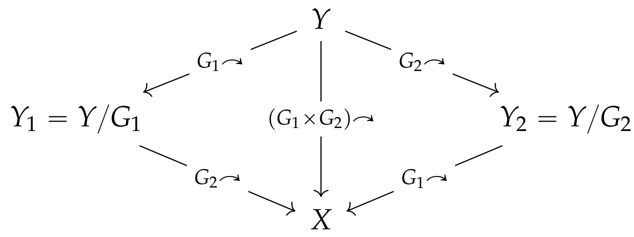
$$U := G/T$$

is k-wound.

Proof. We may extend scalars to assume $k = k_s$, because unipotency commutes with any field extension by Corollary 1.1.12, while the k-wound property and pseudo-reductivity can be verified on a separable closure by Corollary 4.2.4 and Theorem 3.2.2 respectively. In particular, the torus T is k-split. Let us take a k-scheme morphism $f\colon \mathbb{A}^1_k \to U$: by definition, we need to prove that it is constant. Since the fiber product $G \times_U G$ is isomorphic to $T \times G$, the group G is a T-torsor over U. By pulling back via f, the fiber product

$$\begin{array}{ccc} G \times_U \mathbb{A}^1_k & \xrightarrow{pr_1} & \mathbb{A}^1_k \\ \downarrow{\scriptstyle pr_2} & & \downarrow{\scriptstyle f} \\ G & \xrightarrow{\pi} & U \end{array}$$

is a T-torsor over $\mathbb{A}^1_k$, where π denotes the quotient map. Now, for any pair of algebraic groups G_1 and G_2 and any k-scheme X, the following diagram



shows that there is an isomorphism

$$H^1(X, G_1 \times G_2) \longrightarrow H^1(X, G_1) \times H^1(X, G_2)$$
$$Y \longmapsto (Y/G_1, Y/G_2),$$

whose inverse is given by $(Y_1, Y_2) \mapsto Y_1 \times_X Y_2$, where $H^1(X, G)$ denotes the isomorphism classes of G-torsors over X. In our case, since T is split there exists an integer n such that

$$H^1(\mathbb{A}^1_k, T) = H^1(\mathbb{A}^1_k, \mathbb{G}_m^n) \simeq H^1(\mathbb{A}^1_k, \mathbb{G}_m)^n = \mathrm{Pic}(\mathbb{A}^1_k)^n.$$

The Picard group of the affine line is trivial since the ring $k[T]$ is a UFD (see [Rom12, Proposition 4.2.8]), so all T-torsors over $\mathbb{A}^1_k$, and in particular $G \times_U \mathbb{A}^1_k$, must be trivial. This implies the existence of a section $\sigma\colon \mathbb{A}^1_k \to G \times_U \mathbb{A}^1_k$. By setting $\tilde{f} := pr_2 \circ \sigma\colon \mathbb{A}^1_k \to G$, we have the equality $f = \pi \circ \tilde{f}$, so it suffices to prove that $\tilde{f}$ is constant. Up to a translation we may suppose that $\tilde{f}(0) = 1$. We claim the following : for any smooth connected commutative k-group C, and any k-scheme morphism $h\colon \mathbb{A}^1_k \to C$ such that $h(0) = 1$, the smooth connected group H generated by the image of h is unipotent. Applying this to $C = G$ and $h = \tilde{f}$ implies $H = 1$ because G is pseudo-reductive, hence $\tilde{f} = 1$.
In order to prove our claim, we may assume that k is algebraically closed because the formation of H commutes with extension of the ground field (see [Mil17, Proposition 2.47]). In particular, C is the direct product

$$C = \mathbb{G}_m^r \times U'$$

for some integer r and some unipotent k-group U'. Then the projection of H onto U' is clearly unipotent. Hence, by projection onto each factor isomorphic to $\mathbb{G}_m$, we may assume that $C = \mathbb{G}_m$. In particular, the k-algebra homomorphism corresponding to h

$$h^\#\colon k[T, T^{-1}] \longrightarrow k[X]$$

sends T to a nowhere vanishing polynomial $P(X)$ such that $P(0) = 1$, hence we can conclude that $h = 1$. □

4.3 The *cckp*-kernel

Up until this point we have limited ourselves to the study of commutative p-torsion groups. In order to go beyond and study the k-wound property in the general case, we will first look at how those groups embed as k-subgroups of a general smooth connected unipotent group. This means that we will look at subgroups that are smooth, connected, central and p-torsion. Throughout this subsection, U will denote a smooth connected unipotent algebraic group over k and we will specify whether is it supposed to be k-wound or not.

Definition 4.3.1. The *cckp*-**kernel** of U is its maximal smooth connected p-torsion central k-subgroup, which we will denote as $\mathcal{C}_k(U)$.

First, let us notice that this is well-defined: given two such k-subgroups G and H, the algebraic subgroup generated by the multiplication map

$$m_{|G\times H}\colon G\times H\longrightarrow U$$

is still smooth, connected, central and p-torsion.

Remark 4.3.2. Let $U\neq 1$. Since a unipotent algebraic group is nilpotent, as seen in Proposition 1.2.5, its descending central series

$$U=U^0\supset U^1=[U,U^0]\supset\cdots\supset U^i=[U,U^{i-1}]\supset\cdots$$

terminates with 1. Thus, if U^s is its last nontrivial term, it is in particular a smooth central k-subgroup. Since it is commutative, the multiplication by p is well defined. By applying Theorem 1.1.11 to U^s, there exists a minimal $N\geqslant 1$ such that $p^N\cdot U^s=0$. Let us set $H:=p^{N-1}\cdot U^s$: it is a k-subgroup of U^s which is the image of a smooth k-homomorphism, so it is smooth and connected. Moreover, it is nontrivial and p-torsion by minimality of N. Hence U^s contains a nontrivial *cckp*-kernel and we have showed that a nontrivial U has nontrivial *cckp*-kernel.

Lemma 4.3.3. *The formation of the cckp-kernel commutes with separable extensions of the base field: let k'/k be a separable extension and U be a smooth connected unipotent k-group. Then*

$$\mathcal{C}_{k'}(U_{k'})=(\mathcal{C}_k(U))_{k'}.$$

Proof. The proof is based on Galois descent and spreading out of properties from the generic fiber, by using results on limits of schemes, analogously as in the proof of Theorem 3.2.2. □

The following result shows that the k-wound property can actually be verified on the *cckp*-kernel, allowing us to utilise the results found in the preceeding sections.

Proposition 4.3.4. *Let k'/k be a separable field extension. The following are equivalent.*

(1) The group U is k-wound.

(2) The group U does not admit any central k-subgroup isomorphic to $\mathbb{G}_a$.

(3) The subgroup $\mathcal{C}_k(U)$ is k-wound.

(4) The group $U_{k'}$ is k'-wound.

Proof. (1) $\Rightarrow$ (2) : by definition of the k-wound property.
(2) $\Rightarrow$ (3) : Let us assume (3) does not hold, in particular there exists a nontrivial k-scheme morphism $\varphi\colon\mathbb{A}^1_k\to\mathcal{C}_k(U)\subseteq U$. By keeping the notations used in Theorem 3.2.2, since $\mathcal{C}_k(U)$ is commutative

and p-torsion, we can express it as $\mathcal{C}_k(U) = V \times W$. In particular, the vector group V is nontrivial, hence there is a k-subgroup isomorphic to $\mathbb{G}_a$ contained in the *cckp*-kernel of U, which contradicts (2).
(3) $\Rightarrow$ (4) : let us remark that, if $U_{k'}$ is not k'-wound, then (by using results on limits of schemes as in the proof of Theorem 3.2.2) we obtain that the same holds for some finite separable extension K/k. Hence, we ca suppose that k'/k is finite, so $k \subseteq k' \subseteq k_s$ and by Corollary 4.2.4 it suffices to prove that if U_{k_s} is not k_s-wound, then $F := \mathcal{C}_k(U)$ is not k-wound.
Thus, let us consider a nonconstant k_s-scheme morphism $\varphi\colon \mathbb{A}^1_{k_s} \to U_{k_s}$. By composing it with a translation by a rational point we can suppose that $\varphi(0) = 1$. Now, let H be the k_s-subgroup of U_{k_s} generated by φ: we claim that we can suppose H to be central. If this is not true, then in particular U_{k_s} is not commutative. By the smoothness assumption, the k_s-rational points are Zariski-dense, hence there exists $g \in U(k_s)$ not centralizing H. Let us consider the k_s-scheme morphism

$$\varphi^{(1)}\colon \mathbb{A}^1_{k_s} \longrightarrow U_{k_s}, \quad x \longmapsto g^{-1}\varphi(x)^{-1}g\varphi(x),$$

which satisfies $\varphi^{(1)}(0) = 1$ and whose image lies in the derived subgroup $\mathcal{D}(U_{k_s}) = \mathcal{D}(U)_{k_s}$ (see [Mil17, 6.19]). The group U being non commutative, we have $0 < \dim \mathcal{D}(U) < \dim U$. By repeating the same construction, one obtains a sequence of k_s-scheme morphisms $\varphi^{(i)}$ such that each of them is nontrivial and the image of $\varphi^{(i)}$ is contained in the i-th term of the descending central series of U_{k_s}. By nilpotence, we can take the last nontrivial term, whose corresponding morphism $\varphi^{(r)}$ will have an image that is central in U_{k_s}. Moreover, we can obtain such a H that is p-torsion : for this, it is enough to remplace φ by $p^m \cdot \varphi$ for a suitable integer m. This order is bounded thanks to the embedding given by Theorem 1.1.11. Thanks to these assumptions, the nontrivial k_s-subgroup H lies in $\mathcal{C}_{k_s}(U_{k_s})$, which is equal to F_{k_s} by Lemma 4.3.3. In particular, F_{k_s} is not k_s-wound, hence by Corollary 4.2.4, F is not k-wound.
(4) $\Rightarrow$ (1) : a nontrivial k-scheme morphism $\varphi\colon \mathbb{A}^1_k \to U$ gives a nontrivial base change φ_{k_s}. □

Corollary 4.3.5. *Let U be k-wound. Then the quotient*

$$U/\mathcal{C}_k(U)$$

is k-wound.

Proof. Let us denote $F := \mathcal{C}_k(U)$ and notice that by the above proposition we can assume $k = k_s$. Let us assume that U/F is not k-wound, so it contains by (2) a central k-subgroup A that is isomorphic to $\mathbb{G}_a$. Let us consider the following pull-back, where $\pi\colon U \to U/F$ is the canonical projection.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & F & \longrightarrow & \pi^{-1}(A) & \longrightarrow & A & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & F & \longrightarrow & U & \xrightarrow{\pi} & U/F & \longrightarrow & 1 \end{array}$$

The k-subgroup $\pi^{-1}(A)$ is an extension of A by F so it must be smooth, connected and unipotent. Moreover,

- it is central in U : if not, let $g \in U(k_s) = U(k)$ not centralizing $\pi^{-1}(A)$, which exists because the base field is separably closed hence rational points are dense. This allows to define the

k-scheme morphism

$$\varphi\colon \mathbb{A}^1_k \simeq A = \pi^{-1}(A)/F \longrightarrow U, \quad \overline{x} \longmapsto gxg^{-1}x^{-1}$$

which is nonconstant, contradicting the hypothesis that U is k-wound.

- it is p-torsion : if not, we get again a nonconstant scheme morphism

$$\psi\colon \mathbb{A}^1_k \simeq A = \pi^{-1}(A)/F \longrightarrow U, \quad \overline{x} \longmapsto x^p.$$

This shows that $\pi^{-1}(A)$ lies in the *cckp*-kernel F, hence $F = \pi^{-1}(A)$ which implies $A = 1$ and gives a contradiction with the assumption that A is isomorphic to $\mathbb{G}_a$. □

Corollary 4.3.6. *Let U be k-wound and define a chain of smooth connected normal subgroups $\{U_i\}_{i\geqslant 0}$ by setting $U_0 = 1$ and such that U_{i+1} is the pullback*

$$\begin{array}{ccccccccc} 1 & \longrightarrow & U_i & \longrightarrow & U_{i+1} & \longrightarrow & \mathcal{C}_k(U/U_i) & \longrightarrow & 1 \\ & & \| & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & U_i & \longrightarrow & U & \longrightarrow & U/U_i & \longrightarrow & 1. \end{array}$$

Then

(a) If U is k-wound, then so is every U/U_i.

(b) Their formation commutes with separable extensions of k.

(c) For i large enough, $U = U_i$.

(d) These k-subgroups are stable under k-automorphisms of U. In particular, if H is a smooth k-group acting on U, then each U_i is stable under the action of H.

Proof. (a) : Let U be k-wound and proceed by induction on i. For $i = 1$, the quotient $U/U_1 = U/\mathcal{C}_k(U)$ is k-wound by Corollary 4.3.5. Now assume that U/U_i is k-wound and consider the following sequence,

$$1 \longrightarrow U_{i+1}/U_i = \mathcal{C}_k(U/U_i) \hookrightarrow U/U_{i+1} \longrightarrow (U/U_i)/\mathcal{C}_k(U/U_i) \longrightarrow 1,$$

which is exact by definition of the U_is. Now, its kernel $H := U_{i+1}/U_i$ is k-wound by induction and by Proposition 4.3.4, while the quotient $Q := (U/U_i)/\mathcal{C}_k(U/U_i)$ is k-wound again by Corollary 4.3.5. Hence, every k-scheme morphism from the affine line to H and to Q is a constant map to a k-rational point. Since the underlying k-scheme of U/U_{i+1} is the product $H \times Q$, this proves that U/U_{i+1} is wound too.
(b) : By Lemma 4.3.3, the formation on $\mathcal{C}_k$ commutes with separable extensions of the ground field, hence the same is true for each U_i.
(c) : By Remark 4.3.2, if U/U_i is nontrivial then its *cckp*-kernel U_{i+1}/U_i is smooth, connected, unipotent and nontrivial, so it has strictly positive dimension. Since U is algebraic, this implies that U coincides with U_i for a sufficiently large i.

(d) : The stability of U_i under k-automorphisms follows from the fact that they preserve the *cckp*-kernel $\mathcal{C}_k(U)$.
Finally, let H be a smooth k-group acting on U : by the above results, we may extend scalars and assume $k = k_s$. It is enough to prove that U_i is H-stable if $U_i(k)$ is $H(k)$-stable, the latter is a special case of stability under k-automorphisms of U. Let $m\colon H \times U \to U$ denote the action : we want to prove that $m(H \times U_i) \subseteq U_i$ i.e. that

$$H \times U_i \subseteq m^{-1}(U_i) = (H \times U) \times_U U_i.$$

Let us denote respectively $X := H \times U$, $Y := H \times U_i$ and $Z := (H \times U) \times_U U_i$. Both Y and Z are closed subschemes of X and the hypothesis translates into the inclusion $Y(k) \subseteq Z(k)$. Taking their Zariski closures, by definition of reduced subscheme we have $\overline{Y(k)}_{red} \subseteq \overline{Z(k)}_{red}$, which is a subscheme of Z because the underlying topological space of Z is $\overline{Z(k)}$. Moreover, by smoothness of Y we have $\overline{Y(k)}_{red} = Y$ so $Y \subseteq Z$ and we are done. □

The following is a structure theorem, which states exactly what we aimed for when we introduced the notion of k-wound unipotent group : it is analogous to the result of existence of an exact sequence of the form

$$1 \longrightarrow T_s \longrightarrow T \longrightarrow T' \longrightarrow 1,$$

which realizes a torus T as an extension of a k-anisotropic torus $T' = T/T_s$ by the maximal k-split subtorus T_s.

Theorem 4.3.7. *Let U be a smooth connected unipotent k-group. There exists a unique smooth connected normal k-split subgroup U_{split} such that the quotient U/U_{split} is k-wound. It has the following properties:*

(1) If G is a k-split smooth connected unipotent k-group and $\varphi\colon G \to U$ a k-homomorphism, then its image is contained in U_{split}.

(2) If W is a k-wound smooth connected unipotent k-group and $\psi\colon U \to W$ a k-homomorphism, then its kernel contains U_{split}.

(3) The formation of U_{split} is compatible with separable extensions of k.

Proof. Let us proceed by induction on $n = \dim U$, the case $n = 0$ being $U = 1$. If $n > 1$ and U is k-wound, we are done by setting $U_{\text{split}} = 1$. If U is not k-wound, by Proposition 4.3.4 there exists a smooth central k-subgroup $A \simeq \mathbb{G}_a$. Let us denote as H the quotient U/A : by induction there exists a smooth connected normal k-split subgroup H_{split} such that H/H_{split} is k-wound. We call U_{split} its preimage, so that it is an extension of H_{split} by $\mathbb{G}_a$ hence it is k-split. Moreover, the quotient $U/U_{\text{split}} \simeq H/H_{\text{split}}$ is k-wound. Let us prove the properties.
(1) : Consider such a $\varphi\colon G \to U$ and take a composition series $G = G_0 \supset G_1 \supset \cdots \supset G_r = 1$ having successive quotients isomorphic to $\mathbb{G}_a$. Let i be minimal such that $\varphi(G_i) \subseteq U_{\text{split}}$ and suppose $i > 0$. Then the induced morphism

$$\mathbb{G}_a \xrightarrow{\sim} G_{i-1}/G_i \xrightarrow{\overline{\varphi}} U/U_{\text{split}}$$

is nontrivial, contradicting that U/U_{split} is k-wound. Hence $i = 0$ and we are done.
(2) : Consider such a $\psi\colon U \to W$. By applying (1) to W we obtain $\psi(U_{\text{split}}) \subseteq W_{\text{split}} = 1$ which is equivalent to saying $U_{\text{split}} \subseteq \ker \psi$.

(3) : Let k'/k be a separable extension. The k'-subgroup $(U_{\mathrm{split}})_{k'}$ is smooth, connected, normal and k'-split hence it is contained in $(U_{k'})_{\mathrm{split}}$. The quotient $(U_{k'})_{\mathrm{split}}/(U_{\mathrm{split}})_{k'}$ is a k'-split subgroup of $(U/U_{\mathrm{split}})_{k'}$, which is k'-wound because the wound property commutes with separable extensions by Proposition 4.3.4. Thus, it must be trivial and $(U_{k'})_{\mathrm{split}} = (U_{\mathrm{split}})_{k'}$. □

The discussion above leads naturally to introduce the following definition, which is analogous to the unipotent radical.

Definition 4.3.8. Let G be any smooth algebraic group over k. The subgroup $R_{us,k}(G)$ is the maximal **k-split** smooth connected unipotent normal k-subgroup of G.

Notice that this is well defined thanks to [Mil17, Proposition 6.42] : one proceeds in the same way as for the unipotent radical in Corollary 1.1.12.

Corollary 4.3.9. *For any smooth algebraic group G over k,*

$$R_{us,k}(G) = R_{u,k}(G)_{\mathrm{split}}.$$

In particular, the quotient $R_{u,k}(G)/R_{us,k}(G)$ is k-wound and the formation of R_{us} commutes with separable extensions of the base field k.

Proof. For any algebraic field extension k'/k, the subgroup $R_{us,k}(G)_{k'}$ is k'-split hence contained in $R_{us,k'}(G_{k'})$. Now, let us take $k' = k_s$ and consider $R_{us,k_s}(G_{k_s})$. By its uniqueness and maximality, it is invariant by the Galois action so it descends to a k-subgroup H of G, i.e. $H_{k_s} = R_{us,k_s}(G_{k_s})$. Thus, H is necessarily smooth, unipotent and normal in G. Moreover, by Theorem 4.3.7(3), the subgroup H is k-split hence contained in $R_{us,k}(G)$. This gives the inclusion $R_{us,k_s}(G_{k_s}) \subseteq R_{us,k}(G)_{k_s}$. By these observations, we may assume $k = k_s$. The inclusion $R_{us,k}(G) \subseteq R_{u,k}(G)_{\mathrm{split}}$ holds by definition of $R_{us}(G)_{\mathrm{split}}$; conversely, notice that $F := R_{u,k}(G)_{\mathrm{split}}$ is a characteristic k-subgroup of G, hence in particular $F(k)$ is normal in $G(k)$. Since k is separably closed and G is smooth, by Zariski density of its rational points we can conclude that F is normal in G so in particular $F \subseteq R_{us,k}(G)$ and the first statement is proved.
Once we have this equality, the formation of R_{us} is compatible with any separable extension of the ground field because such a compatibility holds

- for the unipotent radical R_u, by Theorem 3.2.2,
- for U_{split}, by Theorem 4.3.7.

□

4.4 Tori acting on unipotent groups

In this last section, the setting will be that of a k-torus acting on a smooth connected unipotent k-group.

Definition 4.4.1. Let T be a k-torus and (V, r) a finite dimensional linear representation of T. If T is k-split, then r is diagonalizable : with respect to a suitable basis of V, it is given by

$$T \longrightarrow \mathrm{GL}_V, \quad t \longmapsto \begin{pmatrix} \chi_1(t) & & 0 \\ & \ddots & \\ 0 & & \chi_n(t) \end{pmatrix}$$

for some characters (eventually admitting repetitions) $\chi_i\colon T \to \mathbb{G}_m$. These characters are called the **weights** of T in V.

Whenever an action of a k-split torus T on an algebraic group G is given, it induces a linear representation of T on the Lie algebra $\mathrm{Lie}(G)$, hence a weight space decomposition, as in Definition 4.4.1, of the latter.
Let us start by the simplest case we are interested in, i.e. assume the unipotent group U equipped with a T-action is a vector group over k, so that $\underline{\mathrm{Lie}(U)} \simeq U$. Recall that a **linear structure** on a vector group V is the $\mathbb{G}_m$-action on it arising from a fixed isomorphism $\mathbb{G}_a^n \simeq V$. The base field being of positive characteristic, there exist nonlinear automorphisms of $\mathbb{G}_a^n$ for $n > 1$, hence the T-action on U may not respect an initial choice of linear structure, as illustrated in the following example.

Example 4.4.2. Let $U = \mathbb{G}_a^2$ with its standard linear structure

$$\mathbb{G}_m \times \mathbb{G}_a^2 \longrightarrow \mathbb{G}_a^2, \quad (a,(x,y)) \longmapsto (ax, ay)$$

and consider $T = \mathbb{G}_m$ acting on U as

$$T \times U \longrightarrow U, \quad (t,(x,y)) \longmapsto t\cdot(x,y) = (tx - (t-t^p)y^p, ty).$$

Clearly, the T-action is not linear. However, by differentiating, since k is of characteristic p, one obtains that the corresponding linear representation of T on $\mathrm{Lie}(U)$ is trivial. Notice that this action becomes linear after composition with the k-group automorphism of $\mathbb{G}_a^2$ given by

$$\alpha\colon \mathbb{G}_a^2 \longrightarrow \mathbb{G}_a^2, \quad \alpha(x,y) = (x+y^p, y), \quad \alpha^{-1}(z,w) = (z - w^p, w).$$

Indeed, for all k-algebras R, we have

$$\alpha^{-1}(t\cdot\alpha(x,y)) = \alpha^{-1}(t\cdot(x+y^p,y)) = \alpha^{-1}(tx + +ty^p - (t-t^p)y^p, ty) = \alpha^{-1}(tx + t^p y^p, ty) = (tx, ty),$$

for all $t \in R^\times = \mathbb{G}_m(R)$ and $x, y \in R^2 = \mathbb{G}_a^2(R)$.

Tits' idea consists in considering an action of a split torus T such that the induced linear representation of T on $\mathrm{Lie}\, U$ has only nontrivial weights, and to deduce from it some properties of the action on the group U. In particular, the existence of such an action imposes some important obstructions on the k-group structure of U.
Let us start, analogously to the preceding sections, by looking at the commutative p-torsion case: later we will proceed with a similar result in the wound case, dropping the assumption of being commutative nor p-torsion. The following proposition is a refinement of Theorem 4.1.12 obtained by adding a given action of a k-group H. Later on, we will restrict to the case of a torus.

Proposition 4.4.3. *Let U be a smooth commutative p-torsion k-group and consider a k-group H acting on U. Then there exists a linear representation of H on a finite dimensional vector space V and an H-equivariant embedding*

$$H \circlearrowright U \xhookrightarrow{\ \psi\ } \underline{V} \circlearrowleft H$$

of U as a k-subgroup of the vector group $\underline{V}$.

Proof. Let us consider the functor

$$\underline{\mathrm{Hom}}(U,\mathbb{G}_a)\colon (\mathrm{k}-\mathbf{Alg}) \longrightarrow (\mathbf{Grp}), \quad R \longmapsto \mathrm{Hom}_{(\mathrm{R}-\mathbf{Grp})}(U_R,\mathbb{G}_{a,R}).$$

Fix a k-algebra R and consider an element of $\underline{\mathrm{Hom}}(U,\mathbb{G}_a)(R)$ i.e. a R-group morphism $\phi\colon U_R \to \mathbb{G}_{a,R}$: it corresponds to a R-linear map $\phi^\# : R[T] \longrightarrow R\otimes_k \mathcal{O}(U)$, which is determined by $f := \phi^\#(T)$. This gives a natural injective map

$$j_R\colon \underline{\mathrm{Hom}}(U,\mathbb{G}_a)(R) \longrightarrow R\otimes_k \mathcal{O}(U), \quad \phi \longmapsto \phi^\#(T). \tag{4.1}$$

Notice that a R-group morphism ϕ corresponds precisely to giving a primitive element in $\mathcal{O}(U_R)$, i.e. to asking that $\phi^\#(T)$ belong to the R-submodule

$$P_R = \{f \in \mathcal{O}(U_R)\colon \Delta_R(f) = f\otimes 1 + 1\otimes f\},$$

where Δ denotes the comultiplication map in $\mathcal{O}(U)$. The condition on f is R-linear and it is functorial in R, so since $k \to R$ is flat, we obtain

$$P_R = P_k \otimes R = \{f \in \mathcal{O}(U)\colon \ = f\otimes 1 + 1\otimes f\}\otimes R.$$

In what follows, we will denote the vector space $P_k = \mathrm{Hom}_{(\mathrm{k}-\mathbf{Grp})}(U,\mathbb{G}_a)$ simply as P. In particular, this shows that

$$\underline{\mathrm{Hom}}(U,\mathbb{G}_a)(R) \simeq \mathrm{Hom}_{(\mathrm{k}-\mathbf{Grp})}(U,\mathbb{G}_a)\otimes R \simeq P\otimes R,$$

so the functor is a vector group associated to the k-vector space P. Now, let us denote the action of H on U as $(h,u) \longmapsto h\cdot u$ and consider the induced action on the k-group scheme $\underline{\mathrm{Hom}}(U,\mathbb{G}_a) = \underline{P}$ given on the functor of points by

$$H(R)\otimes \mathrm{Hom}_{(\mathrm{R}-\mathbf{Grp})}(U_R,\mathbb{G}_{a,R}) \longrightarrow \mathrm{Hom}_{(\mathrm{R}-\mathbf{Grp})}(U_R,\mathbb{G}_{a,R}), \quad (h,\phi) \longmapsto h\cdot\phi$$

with $(h\cdot\phi)(u) := \phi(h^{-1}\cdot u)$ for all $u \in U_R$. The collection of maps j_R defined by 4.1 give a k-group scheme morphism

$$j\colon \underline{\mathrm{Hom}}(U,\mathbb{G}_a) \longhookrightarrow \underline{\mathcal{O}(U)},$$

which we can simply see as being induced by the inclusion of k-vector spaces $P \subset \mathcal{O}(U)$. Since the action we just defined is the restriction of the natural induced action of H on $\mathcal{O}(U)$, it makes j into a H-equivariant morphism.

We now apply the following result (see [CGP15, Proposition A.2.3]): for any k-group G acting on an affine k-scheme X, the coordinate ring $\mathcal{O}(X)$ is the directed union of G-stable finite dimensional k-linear subspaces.

In our case, since j is H-equivariant, we conclude that the same holds for $P = \mathrm{Hom}_{(\mathrm{k}-\mathbf{Grp})}(U,\mathbb{G}_a)$. The group U being smooth, commutative and p-torsion, by Theorem 4.1.12 there exists a k-group closed immersion $i\colon U \longhookrightarrow \mathbb{G}_a^n$ for some $n \geqslant 1$, which corresponds to a k-algebra epimorphism

$$i^\# : k[X_1,\dots,X_n] \longrightarrow \mathcal{O}(U).$$

By the above considerations, we can fix a H-stable finite dimensional k-linear subspace $W \subset P$

containing the set $\{i^\#(X_1), \ldots, i^\#(X_n)\}$, which generates $\mathcal{O}(U)$ as a k-algebra. The k-linear inclusion $W \subset \mathcal{O}(U)$ gives by universal property of the symmetric algebra a H-invariant k-algebra homomorphism

$$\psi^\#: Sym(W) \longrightarrow \mathcal{O}(U),$$

which is surjective by how we defined W and whose corresponding k-scheme morphism

$$\psi: U \longrightarrow \underline{V} := \underline{W^\vee} = \operatorname{Spec}(Sym(W))$$

is thus a closed immersion. Moreover, it is H-invariant because $\psi^\#$ is, and a k-homomorphism because W consists of primitive elements. □

From now on, we will keep the following setting : the group H in Proposition 4.4.3 is assumed to be a k-torus T, acting on the unipotent U admitting a T-equivariant embedding into a vector group $\underline{V}$. The aim is to decompose the vector space V by isolating the part on which the action has only nontrivial weights, in such a way that this decomposition descends to an analogous T-equivariant splitting for the group U.

Proposition 4.4.4. *Within the same setting as in Proposition 4.4.3, let the group H be a k-torus T and consider the T-invariant decomposition of V of the form*

$$V = V_0 \times V',$$

where $V_0 = V^T$ is the subspace fixed by the T-action and V' the span of the isotypic subspaces of the nontrivial irreducible representations of T occurring in V.

(a) The product map

$$m: (U \cap \underline{V_0}) \times (U \cap \underline{V'}) \longrightarrow U$$

is an isomorphism of k-groups.

(b) There is a T-equivariant linear decomposition

$$V' = V_1' \times V_2'$$

and a T-equivariant automorphism α of $\underline{V}$ such that

$$\alpha(U) = (\alpha(U) \cap \underline{V_0}) \times \underline{V_1'}.$$

Proof. (a) : Let us denote $U_0 := U \cap \underline{V_0}$ and $U' := U \cap \underline{V'}$. Since $\underline{V_0} = \underline{V^T} = Z_T(\underline{V})$ and the embedding of U in $\underline{V}$ is T-equivariant, we have $U_0 = Z_T(U)$. Moreover, U is smooth so by [Mil17, Theorem 13.9] the centralizer U_0 is also smooth. If we prove that m is a k-group isomorphism this will imply that U' is smooth too. Consider the vector space V' : it is the span of the vector subspaces

$$V_{\chi_i} := \{v \in V : g \cdot v_R = \chi_i(g) v_R, \ \text{ for all } g \in G(R), \text{ for all } k\text{-algebras } R\},$$

for some nontrivial characters χ_i, so its formation commutes with any extension of the base field and we may assume k to be algebraically closed. In particular, the torus T is split hence the representation $T \to \mathrm{GL}_V$ is a sum of one-dimensional representations. Thus, we can fix a basis $(e_1, \ldots, e_d, f_1, \ldots, f_r)$

of $V = V_0 \times V'$ such that T acts through the character χ_r on kf_i for all $i = 1, \ldots, r$. Since $k = \bar{k}$ and T is smooth, the subset

$$T(k) \setminus ((\chi_1 = 1) \cup \cdots \cup (\chi_r = 1)) \subset T$$

is nonempty, so we can fix a rational point $s \in T(k)$ such that $\chi_i(s) = 1$ for all $i = 1, \ldots, r$. Now, let us consider the k-linear application

$$\varphi \colon V \longrightarrow V, \quad v \longrightarrow s \cdot v - v,$$

which sends V to V' with kernel V_0, because $\varphi(e_j) = 0$ and $\varphi(f_i) = (\chi_i(s) - 1)f_i \neq 0$. By restriction, it defines a linear automorphism of V', hence a k-group automorphism $f \colon \underline{V'} \to \underline{V'}$. Since U is smooth, the image $f(U)$ is a smooth k-subgroup of $\underline{V'}$, which must be contained in U because the embedding of the latter inside of $\underline{V}$ is chosen to be T-stable. Now, let us consider the T-equivariant decomposition

$$V' = kf_1 \oplus \cdots \oplus kf_r,$$

which expresses $\underline{V'}$ as direct sum of one-dimensional vector groups, having nontrivial T-action due to how we chose $s \in T(k)$. In particular, since $f(U)$ is a T-stable k-subgroup of $\underline{V'}$, this decomposition implies that $f(U)$ is connected. Moreover, $U_0 \cap f(U) \subset \underline{V_0} \cap \underline{V'} = 0$, hence the direct product $U_0 \times f(U)$ is a k-subgroup of U. Restricting f to $f(U)$ gives an endomorphism of the latter with trivial kernel, hence a k-group automorphism by smoothness and connectedness. In particular, $f \colon U \to f(U)$ is, up to an automorphism of its image, a quotient map. Since $U \cap \ker f = U \cap \underline{V_0} = U_0$, the inclusion $U_0 \times f(U) \hookrightarrow U$ becomes an isomorphism, and finally

$$f(U) = (U_0 \times f(U)) \cap \underline{V'} = U \cap \underline{V'}$$

and we conclude that m is an isomorphism.
(b) : recall that we have denotes $U' := U \cap \underline{V'}$ and set $V_1' := \mathrm{Lie}(U')$. Since T is k-split, all its linear representations are sum of simple subrepresentations, so the T-stable V_1' admits a T-stable complement V_2' in V'. In particular, the projection

$$\rho \colon U' \longleftrightarrow \underline{V'} \twoheadrightarrow \underline{V_1'}$$

gives an isomorphism $\mathrm{Lie}\,\rho$ on Lie algebras by definition of $\underline{V_1'}$, so as we already argued in previous proofs, the subgroup $H := \ker \rho$ is étale. Moreover, since ρ is T-equivariant, H is T-stable, hence contained in the centralizer $Z_T(V')$, which is trivial by definition of V'. Hence, ρ is an isomorphism. Let us reformulate the inclusion $U' \subset \underline{V'}$ as

$$U \longleftrightarrow \underline{V_1'} \times \underline{V_2'}, \quad x \longmapsto (\rho(x), x - \rho(x)).$$

The second component gives a T-equivariant k-homomorphism

$$g \colon \underline{V_1'} \to \underline{V_2'}, \quad v_1 \longmapsto \rho^{-1}(v_1) - v_1,$$

so we can identify U' with the graph of g inside of $\underline{V'}$. Finally, let us set $\alpha \colon \underline{V} = \underline{V_0} \times \underline{V_1'} \times \underline{V_2'} \longrightarrow \underline{V}$

as being the identity of the factor $\underline{V_0}$ and the inverse of the map

$$(v_1, v_2) \longmapsto (v_1, g(v_1) + v_2)$$

on $\underline{V_1'} \times \underline{V_2'}$. In particular, for $u_0 + x \in U = U_0 \times U'$, since $x = \rho^{-1}(v_1) = (v_1, g(v_1))$ for a unique $v_1 \in \underline{V_1'}$, we have

$$\alpha(u) = u_0 + \alpha(v_1, g(v_1)) = u_0 + v_1 \in U_0 \times \underline{V_1'}$$

as desired. □

In particular, suppose that the linear representation of T on V is sufficiently nontrivial, i.e. that $V_0 = 0$. This implies that $U = U'$, and the T-equivariant automorphism α gives a k-group isomorphism between U and the vector group $\underline{V_1'}$. Thus, the above result has the following consequence.

Corollary 4.4.5. *Let U be a smooth commutative p-torsion k-group and T a k-torus acting on it. Consider a T-equivariant embedding of U into a vector group $\underline{V}$ equipped with a linear representation of T. If $V^T = 0$, then U is a vector group. Moreover, U admits a T-equivariant linear structure.*

Finally, the following result realizes the desired T-equivariant decomposition of the group U, which is independent of any choice of embedding into a vector group.

Theorem 4.4.6. *Let U be a smooth commutative p-torsion k-group equipped with the action of a k-torus T. Then*

$$U = U_0 \times U',$$

with $U_0 = Z_T(U)$ and U' a T-stable subgroup which is a vector group and admits a linear structure relative to which T acts linearly. Moreover, the subgroup U' is uniquely determined and functorial in U.

Proof. The existence of such a $U' = U \cap \underline{V'}$ is given by Proposition 4.4.3 and 4.4.4, so it suffices to prove that it is unique and functorial by finding a description of U' that does not involve any choice of embedding into a vector group $\underline{V}$. For this, we may extend scalars to k_s and suppose k is separably closed. Let us consider a T-equivariant linear structure on the vector group U': the weight space decomposition given by this action must include only nontrivial weights, due to how we defined U_0. In particular, the map

$$T \times U \longrightarrow U, \quad (t, u) \longmapsto t \cdot u - u$$

will have as image the whole U'. This definition only depends on the action of T on U, hence it shows uniqueness and functoriality of U'. □

Let us apply Theorem 4.3.7 to a smooth commutative p-torsion U that is also k-wound. In this case, clearly U' must vanish because a wound group cannot contain any subgroup isomorphic to a vector group: this implies that $U = Z_T(U)$ i.e. the action is necessarily trivial. Actually, the same is still true for any wound group, even without assuming it is commutative nor p-torsion.

Before precisely stating the result, let us introduce a subgroup associated to a cocharacter λ for a smooth connected k-group G, which is an essential element of the proof.

Let $\lambda \colon \mathbb{G}_m \to G$ be a cocharacter : it gives rise to the action by conjugation

$$\mathbb{G}_m \times G \longrightarrow G, \quad (t, g) \longmapsto t \cdot g = \lambda(t) g \lambda(t)^{-1},$$

which induces a linear representation of $\mathbb{G}_m$ on $\operatorname{Lie} G$, hence a weight space decomposition

$$\operatorname{Lie} G = \bigoplus_{n \in X(\mathbb{G}_m) = \mathbb{Z}} (\operatorname{Lie} G)_n = (\operatorname{Lie} G)_- \oplus (\operatorname{Lie} G)_0 \oplus (\operatorname{Lie} G)_+.$$

Definition 4.4.7. Let $g \in G(k)$ be a rational point: we say that the limit $\lim_{t \to 0} t \cdot g$ exists if there is a $\mathbb{G}_m$-equivariant k-scheme morphism $f \colon \mathbb{A}^1_k \to G$ such that $f(1) = g$, where the action of $\mathbb{G}_m$ on the affine line is by scalar multiplication. In other words, this means that we can extend the action of $\mathbb{G}_m$ to the whole $\mathbb{A}^1_k$. If this condition is verified,

$$f(t) = f(t \cdot 1) = t \cdot f(1) = t \cdot g = \lambda(t) g \lambda(t)^{-1}$$

for all $t \neq 0$, and we define the **limit** as $\lim_{t \to 0} t \cdot g := f(0)$.

Now, the following

$$P(\lambda) := \{g \in G \colon \lim_{t \to 0} t \cdot g \text{ exists}\},$$
$$U(\lambda) := \{g \in G \colon \lim_{t \to 0} t \cdot g = 1\} \subseteq P(\lambda)$$

are k-subgroups of G. In particular, $U(\lambda)$ is unipotent and $\operatorname{Lie} U(\lambda) = (\operatorname{Lie} G)_+$; in other words, we have defined a subgroup such that its Lie algebra is the span of the weight spaces having positive weights. For the detailed statements and proofs of these results, see [CGP15, §2.1].
In order to give an idea of what these subgroups look like, let us illustrate the example of the general linear group. The base field k is supposed to be separably closed, because this is the case that will be relevant in the proof.

Example 4.4.8. Let λ be a nontrivial character of GL_n: its image is a smooth connected subgroup of multiplicative type in GL_n and it is different than 1, hence it must be a copy of $\mathbb{G}_m$, in particular contained in a maximal torus. Since all maximal tori are conjugated by a k_s-rational (hence rational since $k = k_s$) point, we may suppose that the image of λ is contained in the maximal torus consisting of invertible diagonal matrices. In particular, there exist integers $a_1, \ldots, a_n$ such that

$$\lambda \colon \mathbb{G}_m \longrightarrow \mathrm{GL}_n, \quad t \longmapsto \begin{pmatrix} t^{a_1} & & 0 \\ & \ddots & \\ 0 & & t^{a_n} \end{pmatrix}$$

Moreover, up to a coordinate permutation we can assume that $a_1 \geqslant \geqslant a_n$. Now, let us fix a rational point $g = (x_{ij})_{i,j=1}^n \in \mathrm{GL}_n(k)$ and consider the element $t \cdot g = \lambda(t) g \lambda(t)^{-1}$: its (i,j)-th coordinate is given by

$$(t \cdot g)_{ij} = \sum_{l,h=1}^{n} \delta_{il} t^{a_i} \delta_{hj} t^{-a_j} = t^{a_i - a_j} x_{ij}.$$

Thus, the limit $\lim_{t \to 0} t \cdot g$ exists if and only if $x_{ij} = 0$ whenever $a_i < a_j$, so the subgroup $P(\lambda)$ consists of all matrices of the form

$$g = (x_{ij})_{i,j} = \begin{pmatrix} B_1 & * & \cdots & * \\ 0 & B_2 & & \vdots \\ \vdots & & \ddots & * \\ 0 & \cdots & 0 & B_m \end{pmatrix},$$

where the blocks B_i are invertible matrices of suitable order such that a new block begins over the column corresponding to an exponent a_j strictly smaller than a_{j-1}. In particular, the limit of such a matrix is

$$\lim_{t \to 0} t \cdot g = \begin{pmatrix} B_1 & 0 & \cdots & 0 \\ 0 & B_2 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & B_m \end{pmatrix},$$

hence the subgroup $U(\lambda)$ corresponds to the matrices having as each B_i the identity matrix of the corresponding order. In this case, we see that $U(\lambda)$ is unipotent and k-split.

Let us come to an end with the following result and its proof; in particular, notice that a fundamental argument is the invariance of the k-wound property with respect to separable field extensions of k, seen in Proposition 4.3.4.

Theorem 4.4.9. *Let T be a k-torus and U a smooth connected unipotent algebraic group over k. If U is k-wound, the only T-action on U is the trivial one.*

Proof. Let us consider an action of T on U and denote its centralizer as Z: our aim is to prove that $Z = U$. Consider the k-group semidirect product $H := U \rtimes T$: by [Mil17, Corollary 13.10], the centralizer $Z_T(G) = Z \rtimes T$ is smooth and connected, hence the same is true for Z. By [CGP15, Corollary A.8.11], since T is of multiplicative type, to prove that $Z = U$ it suffices to prove that $\mathrm{Lie}(Z) = \mathrm{Lie}(U)$, i.e. that T acts trivially on the Lie algebra of U. By Proposition 4.3.4, we can extend scalars and assume that $k = k_s$, so in particular the torus T is k-split. If the T-action on $\mathrm{Lie}(U)$ is nontrivial, there exists a factor isomorphic to the multiplicative group which acts nontrivially, hence we may replace T by such a copy of $\mathbb{G}_m$ and consider a nontrivial 1-parameter subgroup : $\mathbb{G}_m \to U$. By precomposing with the inversion in $\mathbb{G}_m$ if necessary, we can assume there exists a nontrivial weight space in $\mathrm{Lie}\, U$ having a positive weight, i.e. that $(\mathrm{Lie}\, U)_+ \neq 0$. If we consider the semidirect product $G = U \rtimes \mathbb{G}_m$, we can apply the theory briefly illustrated above and consider $U(\lambda) \subset U$: since $\mathrm{Lie}(U(\lambda)) = (\mathrm{Lie}\, U)_+ \neq 0$, in particular it is a nontrivial k-subgroup. It suffices to prove that it is k-split, because this leads to a contradiction with the fact that U is wound. Thus, let us consider the maximal smooth connected normal k-split subgroup $S = U(\lambda)_{\mathrm{split}}$. By Theorem 4.3.7, the quotient $U(\lambda)/S$ is k-wound. Let $g \in U(\lambda)(k)$: by definition of $U(\lambda)$, there is a $\mathbb{G}_m$-equivariant k-scheme morphism $f \colon \mathbb{A}^1_k \to U(\lambda)$ (question why does it go to $U(\lambda)$ and not simply into U?)
such that $f(0) = 1$ and $f(1) = g$. By composing it with the projection $\pi \colon U(\lambda) \to U(\lambda)/S$, we must get a constant map by definition of the wound property, which in particular means that $g = f(1) \in S(k)$. Having assumed the base field to be serparably closed, this is enough to conclude that $U(\lambda) = S$ i.e. that $U(\lambda)$ is split. □

Bibliography

[BLR12] S. Bosch, W. Lütkebohmert, M. Raynaud, **Néron Models**, Vol. 21. Springer Science and Business Media, 2012.

[Bor91] A. Borel, **Linear algebraic groups, Second enlarged edition**, Gra. Texts Math. 126, Springer, 1991.

[CGP15] B. Conrad, O. Gaber, G. Prasad, **Pseudo-reductive groups**,Vol. 26 Cambridge University Press, 2015.

[Con11] B. Conrad, **The structure of solvable groups over general fields**, 2011, available here.

[DG] M. Demazure, P. Gabriel, **Groupes algébriques. Tome I**, Masson and Cie, Éditeur, Paris, North-Holland Publishing Co., Amsterdam, 1970.

[EGA4] A. Grothendieck, **Éléments de géométrie algébrique, Volume 4, Etude locale des schémas et des morphismes de schémas**. IHES, 1964.

[GW] U. Görtz, T. Wedhorn, **Algebraic Geometry I, Schemes with examples and exercises**, Advanced Lectures in Mathematics, Vieweg+Teubner, Wiesbaden, 2010.

[Lei14] T. Leinster, **Basic category theory**, Vol. 143. Cambridge University Press, 2014.

[Mil17] J.S. Milne, **Algebraic groups: the theory of group schemes of finite type over a field**, Cambridge University Press, 2017.

[Neu13] J. Neukirch, **Algebraic number theory**, Vol. 322, Springer Science and Business Media, 2013.

[Oes84] J.Oesterlé, **Nombres de Tamagawa et groupes unipotents en caractéristique p**, Inventiones mathematicae 78.1 (1984), pp. 13–88.

[Rab14] J. Rabinoff, **The theory of Witt vectors**, In: arXiv preprint arXiv:1409.7445 (2014).

[Rom12] M. Romagny, **Géométrie Algébrique 2**, Lecture notes for a Master course at UPMC, 2012, available here.

[SGA3] M. Demazure, A. Grothendieck **Schémas en groupes (SGA 3). Tome II. Groupes de type multiplicatif, et structure des schémas en groupes généraux**, Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3). Lecture Notes in Mathematics 152, Springer-Verlag, 1970.