On the Galois cohomology of unipotent algebraic groups over local and global function fields

Q.T. NGUYEN and D.T. NGUYEN

Institut des Hautes Études Scientifiques
35, route de Chartres
91440 – Bures-sur-Yvette (France)

Août 2005

IHES/M/04/58

On the Galois cohomology of unipotent algebraic groups over local and global function fields

Nguyễn Quốć Thắńg and Nguyễn Duy Tân *

Institute of Mathematics, 18 Hoang Quoc Viet, CauGiay
10307, Hanoi - Vietnam
and
Insitut des Hautes Études Scientifiques, Le Bois-Marie, 35 Rue de Chartres,
F-91440 Bures-sur-Yvette, France

Abstract

We discuss some results on the triviality and finiteness for Galois cohomology of connected unipotent groups over local and global function fields, and their relation with the closedness of orbits. As application, we show that a separable additive polynomial over a global field k of characteristic $p > 0$ in two variables is universal over k if and only if it is so over all completions k_v of k.

AMS Mathematics Subject Classification (2000): Primary 11E72, Secondary 18G50, 20G10

1 Introduction

It is well-known by a result of Rosenlicht [Ro1, 2] that if G is a smooth connected unipotent algebraic group defined over a perfect field k then the group structure of G is very simple : there is a normal series of k-subgroups of G, with each factor isomorphic over k to the additive group $\mathbf{G}_a$ (cf. also

*Supported in part by F. R. P. V., Abdus Salam I. C. T. P. and I. H. E. S. E-mail : nqthang@math.ac.vn, nqt@ihes.fr

[Bo]). In particular, its first Galois cohomology, which will be denoted by $\mathrm{H}^1(k,G) := \mathrm{H}^1(Gal(k_s/k), G(k_s))$, where $Gal(k_s/k)$ denotes the absolute Galois group of k, is trivial (see. e. g. [Se1]). However this is no longer true if k is non-perfect. First Rosenlicht [Ro1, 2] and then Tits [Ti] were able to show certain unusual properties of unipotent groups over non-perfect fields. In [Se1], Chap. III, Serre constructed certain function field k and unipotent k-group G, such that the first Galois cohomology $\mathrm{H}^1(k,G)$ of G is non-trivial (cf. also Raynaud [SGA 3, Exp. 17]). Furthermore, Oesterlé developed in [Oe] a comprehensive arithmetic theory of unipotent groups over global fields and, in particular, showed that the nature of unipotent groups over non-perfect fields is quite non-trivial. One example given there showed that this first cohomology group may be even infinite for some locally compact field of characteristic $p > 0$ (a completion of a global function field). In general, there are many open questions regarding the arithmetic and geometry of unipotent algebraic groups over non-perfect fields. In particular it is interesting to inquire about the Galois cohomology of unipotent groups in this case. Here we are interested in the case where k is a global function field of characteristic $p > 0$. We assume that, unless otherwise stated, all algebraic groups considered here are linear, thus absolutely reduced (i.e., smooth) as in [Bo], [Oe]. We proceed in this paper using some main results from the theory of unipotent groups over non-perfect fields [Oe], [Ro1,2], [Ti] to investigate certain finiteness properties of Galois cohomology of unipotent groups over non-perfect fields and also related local - global principles over global function fields.

Theorem. (cf. Theorem 3.1) *Let k be a global field and let G be a connected smooth unipotent group defined over k. Then the first Galois cohomology group $\mathrm{H}^1(k,G)$ is trivial if and only if it is finite and there is a k-embedding of G into a semisimple (resp. unipotent) smooth simply connected k-group H such that with natural action of H on H/G, the orbits of $H(k)$ are closed in $(H/G)(k)$ in the $A(S)$-topology of $(H/G)(k)$ for any finite set S of valuations of k.*

Theorem. (cf. Theorem 4.8) *Let k be a non-perfect field of characteristic p. Let G be a non-trivial (not necessarily smooth) commutative unipotent k-group scheme of dimension ≤ 1, the connected component G° of which is not k-isomorphic to an extension of $\mathbf{G}_a$ by an infinitesimal k-group scheme. Assume in addition that if $p = 2$ then G° is neither k-isomorphic to an extension of $\mathbf{G}_a$, nor of the subgroup defined as in Proposition 4.2, b), by an*

infinitesimal group scheme. Then the flat cohomology $\mathrm{H}^1_{fl}(k, G)$ *is infinite. In particular, for any global field* k *of positive characteristic and for any non-trivial commutative* k*-unipotent group scheme* G *of dimension* ≤ 1 *with* G° *not* k*-isomorphic to an extension of* $\mathbf{G}_a$*, by an infinitesimal* k*-group scheme, the cohomology set* $\mathrm{H}^1_{fl}(k, G)$ *is infinite.*

Theorem. (cf. Theorem 5.1, Proposition 5.4) (*Local - global principle*) *Let* k *be a global function field and let* G *be a connected smooth unipotent group defined over* k *of dimension* n*.*
a) If n *=1, then* $\mathrm{H}^1(k, G)$ *is trivial if and only if for all valuations* v *of* k *and the completion* k_v *of* k *at* v*,* $\mathrm{H}^1(k_v, G)$ *is trivial.*
b) If $n > 1$*, then Then* $\mathrm{H}^1(k, G)$ *is trivial if and only if for all valuations* v *of* k *and the completion* k_v *of* k *at* v*,* $\mathrm{H}^1(k_v, G)$ *is trivial and there is an embedding of* G *into a smooth* k*-split unipotent group* H *such that with natural action of* H *on* H/G*, the orbits of* $H(k)$ *are closed in* $(H/G)(k)$ *in the* $A(S)$*-topology of* $(H/G)(k)$ *for any finite set* S *of valuations of* k*.*

2 Some definitions and notations

2.1. Recall that a unipotent group G defined over a filed k is called k-wound if any k-morphism of varieties $\mathbf{A}^1 \to G$ is constant. We refer to [Ti], [KMT], [Oe] for detailed discussion of the theory of k-wound groups.

2.2. For a finite field extension K/k and V an affine K-variety, we denote by $R_{K/k}(V)$ the restriction of scalars from K to k. (In the case of separable extension, it is just Weil's restriction of scalars and in the general case, taking into account also the non-separable extension, the definition was given e. g. in [Gr], [DG] or in [Oe], Appendix 3.) For a field k we denote by k_s its separable closure in an algebraic closure $\bar{k}$ of k, $\Gamma = Gal(k_s/k)$ denotes the Galois group of k_s over k, and for a (smooth) linear algebraic k-group G, $\mathrm{H}^1(k, G) := \mathrm{H}^1(\Gamma, G(k_s))$ denotes the first Galois cohomology set of G.

3 Triviality of cohomology and closedness of orbits

Let k be a global field. For a valuation v of k denote by $\mathcal{O}_v$ the ring of v-integers of k_v, and by A the adèle ring of k. Let S be a non-empty finite set of valuations of k, $A(S)$ be the ring of adèles of k with trivial components belonging to S. Then we have for any affine k-variety V,

$$V(A) = \prod_{v \in S} V(k_v) \times V(A(S)),$$

and let $pr_2 : V(A) \to V(A(S))$ be the projection on the second factor. We endow $A(S)$ with the induced topology from the ring of adèles A of k. The induced (from A and $A(S)$) topologies on $V(A)$ and $V(A(S))$ are called adèle and $A(S)$-topology, respectively. Let G be an affine k-group scheme. We say that G satisfies *property* $(*)$ *in dimension* r if the following holds

$(*)$ *For any finite set S of non-equivalent valuations of k, the localization map $\mathrm{H}^r_{fl}(k, G) \to \prod_{v \in S} \mathrm{H}^r_{fl}(k_v, G)$ is surjective*

where H^r_{fl} denotes the flat cohomology group in dimension r, whenever it makes sense (see [Ca], [Mi1,2], [SGA4], [Sh]).
We will see later on that many affine group schemes enjoy this property.

3.1. Theorem. *Let k be a global field and let G be a connected smooth affine group defined over k.*

a) Assume that G satisfies property $(*)$. Then the first Galois cohomology group $\mathrm{H}^1(k, G)$ is trivial if and only if it is finite and for some (thus any) embedding of G into the k-group $H = \mathrm{SL}_n$, such that with natural action of H on H/G, the orbits of $H(k)$ are closed in $(H/G)(k)$ in the $A(S)$-topology of $(H/G)(k)$ for any finite set S containing some fixed finite set S_0 of valuations of k.

b) Assume that G is smooth and unipotent. Then the assertion a) holds where H is either smooth semisimple simply connected k-group or smooth unipotent k-split group.

c) Assume that G is semisimple and either k is a number field or k is a

global function field and the fundamental group of G satisfies the condition $(*)$ in dimension 1. Then the assertion a) holds for semisimple groups G.

Proof. *a*) ("Only if" part.) We take a matrix k-linearization $\varphi : G \hookrightarrow \mathrm{GL}_n$ such that $G \hookrightarrow H := \mathrm{SL}_n$, where GL_n (resp. SL_n) denotes the general (resp. special) linear group of $n \times n$-matrices over k. Then we know that $L = H/G$ is smooth over k and we may consider the following exact sequence

$$1 \to G \to H \to L \to 1.$$

Since H has trivial 1-Galois cohomology (see e.g. [Se1]), so $\mathrm{H}^1(k, H) = 0$, and $\mathrm{H}^1(k_v, H) = 0$, and from [Oe], Chap. III, it follows that $\mathrm{H}^1(\Gamma, H(A(S) \otimes k_s)) = 0$. Since H, G are smooth algebraic groups over k, they are also smooth as A-group schemes and as $A(S)$-group schemes. It follows from [SGA 4] (cf. also [Mi1], Chap. III) that we have canonical isomorphisms between étale cohomology and Galois cohomology

$$\mathrm{H}^i_{et}(A(S), G) \simeq \mathrm{H}^i(\Gamma, G(A(S) \otimes k_s)),$$

$$\mathrm{H}^i_{et}(A(S), H) \simeq \mathrm{H}^i(\Gamma, H(A(S) \otimes k_s)),$$

$$\mathrm{H}^i_{et}(A, G) \simeq \mathrm{H}^i(\Gamma, G(A \otimes k_s)),$$

$$\mathrm{H}^i_{et}(A, H) \simeq \mathrm{H}^i(\Gamma, H(A \otimes k_s)),$$

$(i = 0, 1)$ and we have the following commutative diagrams with exact rows

$$\begin{array}{ccccccccc}
G(k) & \stackrel{i}{\to} & H(k) & \stackrel{r}{\to} & L(k) & \stackrel{\delta}{\to} & \mathrm{H}^1(k, G) & \to & 0 \\
\downarrow & & \gamma \downarrow & & \beta \downarrow & & \alpha \downarrow & & \\
G(A) & \stackrel{i_A}{\to} & H(A) & \stackrel{r_A}{\to} & L(A) & \stackrel{\delta_A}{\to} & \mathrm{H}^1(\Gamma, G(A \otimes k_s)) & \to & 0
\end{array}$$

and

$$\begin{array}{ccccccccc} G(k) & \stackrel{i}{\to} & H(k) & \stackrel{r}{\to} & L(k) & \stackrel{\delta}{\to} & \mathrm{H}^1(k,G) & \to & 0 \\ \downarrow & & \gamma_S \downarrow & & \beta_S \downarrow & & \alpha_S \downarrow & & \\ G(A(S)) & \stackrel{i_S}{\to} & H(A(S)) & \stackrel{r_S}{\to} & L(A(S)) & \stackrel{\delta_S}{\to} & \mathrm{H}^1(\Gamma, G(A(S)\otimes k_s)) & \to & 0 \end{array}$$

where the maps δ, δ_A, δ_S are surjective. By assumption the localization maps are surjective, so from the triviality of $\mathrm{H}^1(k,G)$ it follows the triviality of $\mathrm{H}^1(k_v,G)$ for all v. Thus from [Oe, Ch. I] and from above it follows that $\mathrm{H}^1(\Gamma, G(A(S)\otimes k_s))$ and $\mathrm{H}^1(\Gamma, G(A\otimes k_s))$ are trivial, so r and r_S are surjective. From this the assertion follows.

("If" part.) Assume that $G \hookrightarrow \mathrm{SL}_n$ for some n. We proceed to prove the following lemmas.

3.2. Lemma. *With the notation and assumption in the theorem, for some finite set of valuations S_0 and any finite set S containing S_0,the map α_S is injective.*

Proof. Since H is a semisimple simply connected k-group, it is well-known that there exists a finite set S_0 of valuations such that with respect to S_0, H has the strong approximation in the global field k, i.e., for any finite set S containing S_0, the image $\gamma_S(H(k))$ is dense in $H(A(S))$ in the adèle topology. We may endow $\mathrm{H}^1(k,G)$ and $\mathrm{H}^1(\Gamma, G(A(S)\otimes k_s))$ with weakest topology such that all maps in the above diagram be continuous. Here the sets $G(k), H(k)$ and $L(k)$ are endowed with the topology induced from $G(A(S)), H(A(S)), L(A(S))$, respectively.

Let $x \in \mathrm{Ker}\ (\alpha_S)$ and let $y \in L(k)$ such that $\delta(y) = x$. Then $\delta_S(\beta_S(y)) = 0$, i.e.,

$$\beta_S(y) \in r_S(H(A(S))) = Cl(\beta_S(r(H(k))).$$

Since the adèle topology has a countable basis of topology, there is a sequence $h_n \in H(k)$ such that $\beta_S(r(h_n)) \to \beta_S(y)$ in $A(S)$-topology. Since β_S is just the diagonal embedding $L(k) \hookrightarrow L(A(S))$, it follows that $r(h_n) \to y$ in $L(k)$ in the topology induced from $A(S))$-topology on $L(A(S))$. Hence $\delta(r(h_n)) \to \delta(y)$ in $\mathrm{H}^1(k,G)$. Since $H(k)$-orbits are closed in $L(k)$ with respect to the $A(S)$-topology induced on $L(k)$, and they are finite in number, it follows that all they are open. They are precisely the fibers over elements

of $\mathrm{H}^1(k, G)$. Therefore for sufficiently large n we have $\delta(r(h_n)) = \delta(y)$, so $x = 0$, thus α_S is injective. The lemma is proved.

Next we need the following lemma.

3.3. Lemma. a) *Assume that in the following commutative diagram of pointed topological spaces,*

$$\begin{array}{ccccccc} A & \stackrel{p}{\to} & B & \stackrel{q}{\to} & C & \to & 1 \\ \alpha' \downarrow & & \downarrow \beta' & & \downarrow \gamma' & & \\ A' & \stackrel{p'}{\to} & B' & \stackrel{q'}{\to} & C' & \to & 1 \end{array}$$

where A, A' are topological groups and all maps are continuous and all rows are exact. If $\mathrm{Im}\,(\beta')$ *is dense in B' then so is* $\mathrm{Im}\,(\gamma')$ *in C'.*
b) *If A, A', B, B', C and C' are commutative topological groups,* $\mathrm{Im}\,(\alpha')$ *is dense in* A' *and the closure of the image of* β' *is open in* B'*, then we have the following topological isomorphism*

$$B'/Cl(\mathrm{Im}\,(\beta')) \simeq C'/Cl(\mathrm{Im}\,(\gamma')).$$

Proof. a) Trivial.

b) We have an obvious surjective homomorphism $q' : B' \to C'/Cl(\mathrm{Im}\,(\gamma'))$. Next we show that q' induces a surjective homomorphism

$$\bar{q} : B'/Cl(\mathrm{Im}\,(\beta')) \simeq C'/Cl(\mathrm{Im}\,(\gamma')).$$

For this it suffices to show that

$$q'(Cl(\beta'(B))) \subset Cl(q'(\beta'(B)))(\subset Cl(\mathrm{Im}\,(\gamma'))).$$

Let $b' \in Cl(\beta'(B))$, V an arbitrary open neighborhood of $q'(b')$ in C'. We need to show that $V \cap q'(\beta'(B))) \neq \emptyset$. Since q' is continuous, $q'^{-1}(V)$ is open in B', which contains b'. Hence $q'^{-1}(V) \cap \beta'(B) \neq \emptyset$. Let $y \in q'^{-1}(V) \cap \beta'(B)$, so $q'(y) \in V \cap q'(\beta'(B))$, so $V \cap q'(\beta'(B))) \neq \emptyset$ as required.

Next we show that $\mathrm{Ker}\,(\bar{q}) = 0$. It is clear that this amounts to proving that

$$q'^{-1}(Cl(\gamma'(C)) = Cl(\beta'(B)).$$

Clearly the set on the left contains the one on the right, since $q'^{-1}(Cl(\gamma'(C)))$ is closed and containing $\mathrm{Im}\,(\beta')$). Notice that

$$q'^{-1}(Cl(\gamma'(C)) = q'^{-1}(Cl(\gamma'(\beta'(B))))$$

$$= q'^{-1}(Cl(q'(\beta'(B)))),$$

hence it suffices to show that $Cl(q'(\beta'(B))) \subset q'(Cl(\beta'(B)))$. Indeed, assuming that this inclusion holds. Then one has

$$q'^{-1}(Cl(q'(\text{Im } \beta'))) \subset q'^{-1}(q'(Cl(\text{Im } \beta')))$$

$$= p'(A')Cl(\text{Im } \beta').$$

Since Im α' is dense in A' so we have

$$p'(A') = p'(Cl(\alpha'(A)))$$

$$\subset Cl(p'(\alpha'(A)))$$

$$= Cl(\beta'(p(A)))$$

$$\subset Cl(\beta'(B)),$$

hence we have $q'(Cl(\beta'(B))) \subset Cl(q'(\beta'(B)))$ as claimed. Since $Cl(\beta'(B))$ is open in B' and q' is an open map (as quotient homomorphism), it follows that $q'(Cl(\beta'(B)))$ is an open subgroup of C', hence also a closed subgroup. It contains $q'(\beta'(B))$, hence also $Cl(q'(\beta'(B)))$ as required. The lemma is proved.

Next we prove that the image of $\mathrm{H}^1(k, G)$ in $\mathrm{H}^1(\Gamma, G(A(S) \otimes k_s))$ is trivial for S sufficiently large. First we introduce some notations. If char.$k = 0$, let $\mathcal{O}$ be the ring of integers of k, $\mathcal{C} = \text{Spec}\mathcal{O}$, and if char.$k > 0$, let $k = \mathbf{F}(\mathcal{C})$, which is the function field of a geometrically integral smooth curve $\mathcal{C}$ over a finite field $\mathbf{F}$. One may find an affine group scheme $\mathcal{G}_{\mathcal{C}'}$ of finite type over an open affine subset $\mathcal{C}' \subset \mathcal{C}$, such that G is k-isomorphic to the generic fiber of $\mathcal{G}_{\mathcal{C}'}$. The following argument is in fact a "folklore", which follows from results of [EGA IV] (cf [Oe]). It is well-known that the subset $\mathcal{C}' \subset \mathcal{C}$ of all elements $c \in \mathcal{C}$ where the canonical morphism $\mathcal{G}_{\mathcal{C}} \to \mathcal{C}$ is smooth, is open (in this case we just need Zariski's result [EGA IV], 0.22.6.8 and 17.5.1). By passing to an affine open subset $\mathcal{C}'' \subset \mathcal{C}'$ and use [EGA IV], 17.8.2, we see that all fibers over $s \in \mathcal{C}''$ are smooth. Now $\mathcal{G}_{\mathcal{C}''} \to \mathcal{C}''$ is smooth and of finite type and also finite presentation. By [EGA IV], 9.7.8, over a suitable open and

non-empty subset $\mathcal{C}''' \subset \mathcal{C}''$, all fibers will be also geometrically connected, since by assumption G is connected. Thus over $\mathcal{C}'''$, all fibers are smooth and connected group schemes.

Thus, after shrinking $\mathcal{C}'$ we may assume that all fibers of $\mathcal{G}_{\mathcal{C}'}$ are smooth, connected affine groups. Every G-torsor P over k (i.e. principal homogeneous space of G) comes from certain $\mathcal{G}_{\mathcal{C}'}$-torsor $P_{\mathcal{C}'}$ for suitable $\mathcal{C}'$ (depending on P). Since $\mathrm{H}^1(k, G)$ is finite by assumption, we may take $\mathcal{C}'$ sufficiently small, so that for such $\mathcal{C}'$, every G-torsor P comes from a $\mathcal{G}_{\mathcal{C}'}$-torsor $P_{\mathcal{C}'}$. For every closed point $s \in \mathcal{C}'$ let $v(s)$ be the corresponding valuation with the local ring $\mathcal{O}_{v(s)}$, the maximal ideal $m_{v(s)}$, the completion $k_{v(s)}$ (of k at $v(s)$) and the finite residue field $\kappa(v(s))$. We have the following commutative diagram

$$\begin{array}{ccc}
\mathrm{H}^1_{et}(\mathcal{C}', \mathcal{G}_{\mathcal{C}'}) & \to & \mathrm{H}^1_{et}(\mathrm{Spec}\ k, \mathcal{G}_{\mathcal{C}'} \times_{\mathcal{C}'} \mathrm{Spec}\ k) \\
\downarrow & & \downarrow \\
\mathrm{H}^1_{et}(\mathrm{Spec}\ \mathcal{O}_{v(s)}, \mathcal{G}_{\mathcal{C}'} \times_{\mathcal{C}'} \mathrm{Spec}\ \mathcal{O}_{v(s)}) & \to & \mathrm{H}^1_{et}(\mathrm{Spec}\ k_{v(s)}, \mathcal{G}_{\mathcal{C}'} \times_{\mathcal{C}'} \mathrm{Spec}\ k_{v(s)}) \\
\downarrow f & & \\
\mathrm{H}^1_{et}(\mathrm{Spec}\ \kappa(v(s)), \mathcal{G}_{\mathcal{C}'} \times_{\mathcal{C}'} \mathrm{Spec}\ \kappa(v(s))) & &
\end{array}$$

and for a $\mathcal{G}_{\mathcal{C}'}$-torsor $P_{\mathcal{C}'}$ we have

$$\begin{array}{ccc}
P_{\mathcal{C}'} & \mapsto & P := P_{\mathcal{C}'} \times_{\mathcal{C}'} \mathrm{Spec}\ k \\
\downarrow & & \downarrow \\
P_{\mathcal{C}'} \times_{\mathcal{C}'} \mathrm{Spec}\ \mathcal{O}_{v(s)} & \mapsto & P_{k_{v(s)}} := P \times_{\mathrm{Spec}\ k} \mathrm{Spec}\ k_{v(s)} \\
\downarrow & & \\
P_{\mathcal{C}'} \times_{\mathcal{C}'} \mathrm{Spec}\ \kappa(v(s)) & &
\end{array}$$

which shows that $P_{k_{v(s)}}$ is isomorphic to the generic fiber of $P_{\mathcal{C}'} \times_{\mathcal{C}'} \mathrm{Spec}\ \mathcal{O}_{v(s)}$. Now every closed fiber of $\mathcal{G}_{\mathcal{C}'}$ is a smooth and connected algebraic group and defined over a finite field, hence by Lang's Theorem (see [La]), it has trivial Galois cohomology. Therefore every closed fiber $P_{\mathcal{C}'} \times_{\mathcal{C}'} \mathrm{Spec}\ \kappa(v(s))$ of $\mathcal{G}_{\mathcal{C}'}$-torsor $P_{\mathcal{C}'}$ is a trivial torsor. Since $\mathcal{G}_{\mathcal{C}'}$ is smooth, from "Hensel Lemma" (see Grothendieck [SGA 3, Exposé. XXIV, Prop. 8.1, (ii)]) it follows that f is an isomorphism, so $P_{\mathcal{C}'} \times_{\mathcal{C}'} \mathrm{Spec}\ \mathcal{O}_{v(s)}$ (hence also $P_{k_{v(s)}}$) is trivial. From [Oe], Chap. III, Sec. 2.4, it follows that

$$\mathrm{H}^1(\Gamma, G(A(S) \otimes k_s)) \simeq \coprod_{v \notin S} \mathrm{H}^1(k_v, G).$$

Therefore by taking $\mathcal{C} \setminus \mathcal{C}'$ (hence also $S = \{v(s) | s \in \mathcal{C} \setminus \mathcal{C}'\}$) sufficiently large, we see that the image of $\mathrm{H}^1(k, G)$ in $\mathrm{H}^1(\Gamma, G(A(S) \otimes k_s))$ is trivial and the assertion a) of the theorem follows.

b) If char.$k = 0$, then the first Galois cohomology of unipotent groups is trivial, and "only if" part needs proving, but this follows from above. Now we assume that char.$k > 0$. Smooth unipotent groups over any field satisfy the property $(*)$ by [TT], so the assertion related with semisimple simply connected groups is coved in part a), and the rest follows from the fact that k-split unipotent groups have strong approximation over k for any S.
(In the case H is a unipotent group, we have a shorter argument as follows. Let H be a k-split unipotent group. The "only if" part is proved like above. Conversely, we show that $\mathrm{H}^1(k, G)$ is trivial. Since H is unipotent and k-split, the quotient space L is k-isomorphic to the affine space $\mathbf{A}^r$ for some r (see [Ro1],[Ro 2]). Hence L has strong approximation, thus the closure $Cl(\beta_S(L(k)))$ is equal to $L(A(S))$. Therefore α_S is surjective by Lemma 3.3. Since $\mathrm{H}^1(k, G)$ is finite, it follows that $\mathrm{H}^1(\Gamma, G(A(S) \otimes k_s))$ is finite, too. From [Oe], Chap. III, Sec. 2.4, it follows that

$$\mathrm{H}^1(\Gamma, G(A(S) \otimes k_s)) \simeq \coprod_{v \notin S} \mathrm{H}^1(k_v, G),$$

hence for all $v \notin S$, $\mathrm{H}^1(k_v, G)$ is finite and for almost all v, $\mathrm{H}^1(k_v, G)$ is trivial. Let $S_0 := \{v | \mathrm{H}^1(k_v, G) \neq 0\}$. Then S_0 is finite and for $S = S_0$, according to Lemma 3.2, we have an injection

$$\mathrm{H}^1(k, G) \to \mathrm{H}^1(\Gamma, G(A(S) \otimes k_s)) \simeq \coprod_{v \notin S} \mathrm{H}^1(k_v, G) = \{0\},$$

thus $\mathrm{H}^1(k, G)$ is trivial, too.

c) Now we assume that k is a number field. Then Borel and Harder have proved ([BH], Theorem 1.7), that G satisfies the property $(*)$. We give here a modification of their proof. Consider the k-covering of G, i.e., a semisimple simply connected k-group H together with the following exact sequence

$$1 \to F \to H \to G \to 1,$$

where F is a finite diagonalizable k-subgroup of H. We have the following commutative diagram, where each row is an exact sequence of Galois cohomology

$$\begin{array}{ccccccc}
\mathrm{H}^1(k, F) & \to & \mathrm{H}^1(k, H) & \stackrel{\pi}{\to} & \mathrm{H}^1(k, G) & \stackrel{\Delta}{\to} & \mathrm{H}^2(k, F) \\
\downarrow & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma \\
\prod_{v\in S} \mathrm{H}^1(k_v, F) & \to & \prod_{v\in S} \mathrm{H}^1(k_v, H) & \stackrel{\pi_S}{\to} & \prod_{v\in S} \mathrm{H}^1(k_v, G) & \stackrel{\Delta_S}{\to} & \prod_{v\in S} \mathrm{H}^2(k_v, F)
\end{array}$$

We take any sufficiently large finite set S of (non-equivalent) valuations of k such that S contains the set of all archimedean valuations ∞ of k. Then the well-known Hasse principle for simply connected groups (see [PR], for the case of number fields, and [Ha], for the case of function field) tells us that α is bijective, and a result of [BH], Proposition 1.6, says that γ is surjective. Also, classical results due to Kneser [Kn] (for the case of number field), and [T] (for the case of function field), say that Δ and Δ_S are surjective. Thus by chasing on the above diagram we see that for any given $g_S \in \prod_{v\in S} \mathrm{H}^1(k_v, G)$ there is an element $g \in \mathrm{H}^1(k, G)$ such that

$$\Delta_S(g_S) = \Delta_S(\beta(g))).$$

By twisting the exact sequence

$$1 \to F \to H \to G \to 1$$

with a cocycle (x_s) representing the class g we get another exact sequence

$$1 \to F \to {}_xH \to {}_xG \to 1.$$

By considering the commutative diagram with rows being exact sequences of Galois cohomology deduced from this exact sequence as above, we are

reduced to the case $g = 0$ (the distinguished element in $\mathrm{H}^1(k, G)$. Then $\Delta_S(g_S) = 0$, i.e., $g_S = \pi_S(h_S)$ for some element $h_S \in \prod_{v \in S} \mathrm{H}^1(k_v, H)$, hence, by using the surjectivity of α, we deduce that $g_S \in \mathrm{Im}\,(\beta)$ as required.

In the case of global function fields, by using the fact that H^1 of simply connected groups is trivial (Harder' Theorem [Ha])

$$\mathrm{H}^1_{fl}(k, G) \to \mathrm{H}^2_{fl}(k, F)$$

is a bijection ([T]), the condition $(*)$ in dimension 2 for F then means that the same holds for G in dimension 1. ∎

3.4. Corollary. *Let G be a smooth unipotent group defined over a global field k. Then for any non-empty finite set S of non-equivalent valuations of k, the restriction map*

$$\mathrm{H}^1(k, G) \to \coprod_{v \notin S} \mathrm{H}^1(k_v, G)$$

is surjective.

Proof. We may embed G into a smooth k-split unipotent group H and then consider the exact sequence

$$1 \to G \to H \to L \to 1,$$

and the related diagram as in Lemma 3.2. We now apply Lemma 3.3, noticing that L has strong approximation over k with respect to any finite non-empty S. ∎

4 Finiteness for Galois cohomology of unipotent groups

In this section we prove some criteria for the finiteness of Galois cohomology of unipotent groups over non-perfect fields. A special attention is devoted to the case of local and global function fields. The following simple lemma which is well-known [We] but we give here another short proof.

4.1. Lemma. *Let k be a global (local) function field of characteristic $p > 0$.*

Then $[k : k^p] = p$.

Proof. We claim that if k is a field of char p and $[k : k^p] = p$ then $[k' : k'^p] = p$, for all finite extensions k' over k. If $\{x_1, \ldots, x_n\}$ is a basis of k' over k then $\{x_1^p, \ldots, x_n^p\}$ is a basis of k'^p over k^p. Therefore, $[k' : k] = [k'^p : k^p]$, and we have

$$[k' : k'^p] = \frac{[k' : k][k : k^p]}{k'^p : k^p} = [k : k^p].$$

We first prove the lemma for the case $k = \mathbf{F}_q(t)$, t is transcendental over $\mathbf{F}_q$. Let $P(T)$ be an arbitrary polynomial in $\mathbf{F}_q[T]$. Then we can write $P(T) = \sum_{i=0}^{p-1} T^i P_i^p(T)$. An element $a \in k$ is always of form $a = \frac{P(t)}{Q(t)}, P(T), Q(T) \in \mathbf{F}_q[T]$. We have

$$a = \frac{P(t)}{Q(t)} = \frac{P(t)Q(t)^{p-1}}{Q^p(t)} = \sum_{i=0}^{p-1} t^i \left(\frac{R_i(t)}{Q(t)}\right)^p.$$

So $\{1, t, \ldots, t^{p-1}\}$ generates k over k^p (as a vector over k^p). Since t is transcendental over $\mathbf{F}_q$, $\{1, t, \ldots, t^{p-1}\}$ is linearly independent over k^p. Hence, $\{1, t, \ldots, t^{p-1}\}$ is a basis of k over k^p, and $[k : k^p] = p$.

So from above it follows that the lemma is true for global fields.

Now, consider the case of local fields of characteristic $p > 0$. We may assume $k = \mathbf{F}_q((t))$. Let $a = \sum_{i \geq i_0} a_i t^i, a_i \in \mathbf{F}_q$ be an element of k. Since every elements of $\mathbf{F}_q$ is a p-power, we can write $a_i = b_i^p$, $b_i \in \mathbf{F}_q$. Therefore, we get

$$\begin{aligned} a &= \sum_{i \geq i_0} b_i^p t^i \\ &= \sum_{r=0}^{p-1} \sum_{i \geq (i_0 - r)/p} b_{pi+r}^p t^{pi+r} \\ &= \sum_{r=0}^{p-1} t^r \left(\sum_{i \geq (i_0 - r)/p} b_{pi+r} t^{pi+r} \right)^p \\ &= \sum_{r=0}^{p-1} t^r a_r^p, \end{aligned}$$

where $a_r \in k$. Hence, $\{1, t, \ldots, t^{p-1}\}$ generates k over k^p. And $1, t, \ldots, t^{p-1}$ are linearly independent over k^p, so $\{1, t, \ldots, t^{p-1}\}$ is a basis of k over k^p and $[k : k^p] = p$. ∎

Next we examine a class of unipotent groups of special type over non-perfect fields of characteristic $p > 0$, namely the groups defined by the following equation

$$x_0^p + tx_1^p + \cdots + t^{p-1}x_{p-1}^p - x_{p-1} = 0.$$

This class of groups was first considered by Rosenlicht in [Ro1,2], and then in [KMT], [Oe], [Ti], where they served as simple but important examples, which will be needed in the sequel. First we consider the case of characteristic 2.

4.2. Proposition. *a) Let k_v be $\mathbf{F}_q((t))$, $q = 2^n$, G the $\mathbf{F}_p(t)$-subgroup of $\mathbf{G}_a^2$ defined by the equation $y^2 = x + tx^2$. Then $|\mathrm{H}^1(k_v, G)| = 2$.*
b) Let k be a global function field of characteristic 2, t an element of $k - k^2$. Let G be the closed subgroup of $\mathbf{G}_a^2$ defined as above. For v a nontrivial valuation of k, let k_v be the completion of k with respect to v. Then $|\mathrm{H}^1(k_v, G)| = 2$, and $\mathrm{H}^1(k, G)$ is infinite.

Proof. Let $P(x, y) = y^2 + x + tx^2$, and consider P as a homomorphism from $\mathbf{G}_a^2$ to $\mathbf{G}_a$. We have an exact sequence of unipotent k-groups

$$1 \to G \to \mathbf{G}_a^2 \xrightarrow{P} \mathbf{G}_a \to 1.$$

From this we have $\mathrm{H}^1(k_v, G) \simeq k_v/P(k_v \times k_v)$ since $\mathrm{H}^1(k_v, \mathbf{G}_a) = 0$.

a) First, we show that

(1) $\quad ct^{-i} \in P(k_v \times k_v)$, *for all* $c \in \mathbf{F}_q, i \geq 2$,

by induction on i. In fact, if $c = \alpha^2$, where $\alpha \in \mathbf{F}_q$, then $ct^{-2i} = P(0, \alpha t^{-i})$. Since any element of $\mathbf{F}_q$ is a square, it follows that the statement holds for all even numbers i. Assume that (1) holds for all numbers j with $2 \leq j \leq i$. If i is odd, then $i + 1$ is even and from above we know that (1) holds for $i + 1$, so we are done. If i is even ≥ 2, $i = 2j$, then $2 \leq j < i - 1$ and by induction assumption, there are $a, b \in k_v$ such that $\alpha t^{-j-1} = P(a, b)$ where

$c = \alpha^2$, with $\alpha \in \mathbf{F}_q$, and $a, b \in k$. Then we have $ct^{-2j-1} = P(a + \alpha t^{-j-1}, b)$. Hence (1) also holds for $i + 1 = 2j + 1$.

Next, we prove that

(2) $\mathbf{F}_q[[t]] \subset P(k_v \times k_v),$, *i.e.* $\sum_{i \geq 0} c_i t^i \in P(k_v \times k_v), \forall c_i \in \mathbf{F}_q$.

In fact, if we can find $y \in \mathbf{F}_q[[t]]$ such that

$$y^2 + dy/dt = \sum_{i \geq 0} c_{2i+1} t^{2i}, \tag{3}$$

where (d/dt) denotes the differentiation with respect to t, then

$$s = ty^2 + y + \sum_{i \geq 0} c_i t^i = x^2,$$

for some $x \in \mathbf{F}_q[[t]]$, since $ds/dt = 0$. Now, by writing $y = \sum_{i \geq 0} y_i t^i$ and by substituting it into the left hand side of the equation (3), we have

$$\begin{aligned} y^2 + dy/dt &= \sum_{i \geq 0} y_i^2 t^{2i} + \sum_{i \geq 0} y_{2i+1} t^{2i} \\ &= \sum_{i \geq 0} (y_i^2 + y_{2i+1}) t^{2i}. \end{aligned}$$

By comparing those coefficients with the same power of t in (3) we derive

$$y_i^2 + y_{2i+1} = c_{2i+1}, \forall i \geq 0$$

and by setting $y_{2i} = 1, y_{2i+1} = c_{2i+1} + y_i^2$, we get a solution for (3).

Finally, we claim that

(4) *for any $\alpha \in \mathbf{F}_q$, then $\alpha t^{-1} \in P(k_v \times k_v)$ if and only if $\alpha = u^2 + u$, for some $u \in \mathbf{F}_q$.*

In fact, if $\alpha t^{-1} = b^2 + a + ta^2$, for some $a, b \in k$, then by differentiating both sides with respect to t, we get $\alpha t^{-2} = da/dt + a^2$. It suffices to consider the case when $\alpha \neq 0$. In this case, $a \neq 0$, and we can write $a = t^l u$, where $l \in \mathbf{Z}, u \in k, v_t(u) = 0$, and v_t denotes the valuation corresponding to t. Then

(5) $$\alpha t^{-2} = lt^{l-1}u + t^l du/dt + t^{2l}u^2.$$

We have

$$v_t(lt^{l-1}u + t^l du/dt + t^{2l}u^2) \geq 0$$

if $l \geq 0$, and

$$v_t(lt^{l-1}u + t^l du/dt + t^{2l}u^2) = 2l \leq -4$$

if $l \leq -2$. Therefore, by comparing both sides of (5), we see that l equals -1, and by writing $u = u_0 + tu_1$, $u_0 \in \mathbf{F}_q, u_1 \in \mathbf{F}_q[[t]]$, we get $\alpha = u_0^2 + u_0$. Evidently, if $\alpha = u^2 + u$, for some $u \in \mathbf{F}_q$, then $\alpha t^{-1} = P(ut^{-1}, 0)$.

From (1), (2), (4) and by observing that the map $u \mapsto u^2 + u$ is a homomorphism from $(\mathbf{F}_q, +)$ to $(\mathbf{F}_q, +)$ with kernel $\mathbf{F}_2$, we conclude that $|\mathrm{H}^1(k_v, G)| = 2$ and the assertion is proved.

b) Let π be a prime (uniformizing element) for v. For simplicity, we identify k_v with the field $k(v)((\pi))$, where $k(v)$ is the residue field of k respect to v, so $k(v) = \mathbf{F}_q$, with $q = 2^n$. By Lemma 4.1, we can write $t = a^2 + \pi b^2$, $a, b \in k_v$. It is easy to check that $b \neq 0$. By making the change of variables $y' = b(y + ax), x' = b^2 x$, one checks that G is isomorphic to the subgroup

$$G' = \{y'^2 = x' + \pi x'^2\}.$$

Therefore from part *a*) it follows that $|\mathrm{H}^1(k_v, G)| = |\mathrm{H}^1(k(v)((\pi)), G')| = 2$. We know that the localization map

$$\mathrm{H}^1(k, G) \to \prod_{v \in F} \mathrm{H}^1(k_v, G)$$

is surjective for any finite set F of non-equivalent discrete valuations ([TT]). Since there are infinitely many v, we conclude that $\mathrm{H}^1(k, G)$ is infinite. ∎

For the case $p > 2$, we have the following result. The idea of the proof is similar to the above one, but the computation is more complicated, so we give a full proof.

4.3. Proposition. *a*) *Let $k = \mathbf{F}_q(t)$, v be the valuation corresponding to t and $k_v = \mathbf{F}_q((t)), q = p^n, p > 2$. Let G be the $\mathbf{F}_p(t)$-subgroup of $\mathbf{G}_a^p$ defined by the equation $x_0^p + tx_1^p + \cdots + t^{p-1}x_{p-1}^p = x_{p-1}$. Then $|\mathrm{H}^1(k_v, G)| = p$.*
b) *Let k be a global function field of characteristic $p > 2$, t an element in*

$k - k^p$. Let G be the subgroup of $\mathbf{G}_a^p$ defined as above. Then for infinitely many non-equivalent valuations v of k, $\mathrm{H}^1(k_v, G) \neq \{1\}$ and $\mathrm{H}^1(k, G)$ is infinite.
c) Let $k_v = \mathbf{F}_q((t))$, $q = p^n, p > 2$. Let G be the $\mathbf{F}_p(t)$-subgroup of $\mathbf{G}_a^p$ defined by the equation $x_0^p + tx_1^p + \cdots + t^{p-1}x_{p-1}^p + x_{p-1} = 0$. Then $|\mathrm{H}^1(k_v, G)| = 1$ (resp. p) if n is odd (resp. even).

Proof. *a*) We first show that for

$$P(x_0, ..., x_{p-1}) = x_0^p + tx_1^p + \cdots + t^{p-1}x_{p-1}^p - x_{p-1}$$

then

(1) $\quad ct^{-i} \in P(k_v \times \cdots \times k_v)$, *for all* $c \in \mathbf{F}_q, i \geq 2$,

by induction on i. Since any element of $\mathbf{F}_q$ is a p-power, we may write $c = \beta^p, \beta \in \mathbf{F}_q$. We have, for $0 \leq r \leq p-1, r \neq 1$,

$$ct^{-(pl+r)} = P(0, \ldots, \beta t^{-l-1}, \ldots, 0),$$

where all coordinates are 0 except at x_{p-r}. Assume that (1) holds for all numbers j, with $2 \leq j \leq i$. If $i \not\equiv 0 \pmod{p}$, then $i + 1 \not\equiv 1 \pmod{p}$, so $i + 1 = pl + r$, where $0 \leq r \leq p-1, r \neq 1$, so (1) holds for $i + 1$, and we are done. If $i = pj$ then $2 \leq j < i$ and by induction assumption, there are $a_0, \ldots, a_{p-1} \in k_v$ such that $\beta t^{-(j+1)} = P(a_0, \ldots, a_{p-1})$. By setting

$$x_0 = a_0, \ldots, x_{p-2} = a_{p-2}, x_{p-1} = a_{p-1} + \beta t^{-(j+1)},$$

we have

$$\begin{aligned} x_0^p + tx_1^p + \cdots + t^{p-1}x_{p-1} - x_{p-1} &= (a_0^p + ta_1^p + \cdots + t^{p-1}a_{p-1}^p - a_{p-1}) \\ &\quad + t^{p-1}(\beta t^{-(j+1)})^p - \beta t^{-(j+1)} \\ &= (P(a_0, ..., a_{p-1}) - \beta t^{-(j+1)}) + (\beta^p t^{-(pj+1)}) \\ &= ct^{-(pj+1)}. \end{aligned}$$

Next, we prove that

(2) $\mathbf{F}_q[[t]] \subset P(\mathbf{F}_q[[t]] \times \cdots \times \mathbf{F}_q[[t]])$, i.e., for all $c_i \in \mathbf{F}_q$ we have

$$c(t) := \sum_{i \geq 0} c_i t^i \in P(\mathbf{F}_q[[t]] \times \cdots \times \mathbf{F}_q[[t]]).$$

In fact, by differentiating with respect to t both sides of the following equation

$$\sum_{i \geq 0} c_i t^i = x_0^p + t x_1^p + \cdots + t^{p-1} x_{p-1}^p - x_{p-1}$$

$(p-1)$ times, and by observing that $(p-1)! \equiv -1 \pmod{p}$ (Wilson's theorem), we get

$$d^{p-1}c(t)/dt^{p-1} = \sum_{i \geq 0} c_{pi+p-1} t^{pi} = x_{p-1}^p - d^{p-1}x_{p-1}/dt^{p-1}. \tag{3}$$

First we find x_{p-1} satisfying (3) as follows. Let $x_{p-1} = \sum_{i \geq 0} y_i t^i$ then

$$x_{p-1}^p - d^{p-1}x_{p-1}/dt^{p-1} = \sum_{i \geq 0} (y_i^p - y_{pi+p-1}) t^{pi}.$$

Using this and by comparing those coefficients with the same power of t in (3), we get

$$y_i^p - y_{pi+p-1} = c_{pi+p-1}, \forall i \geq 0.$$

By setting $y_{pi+r} = 0$, $0 \leq r \leq p-2$, $y_{pi+p-1} = y_i^p - c_{pi+p-1}$, we get a solution x_{p-1} for (3). From this it follows that

$$\frac{d}{dt}\left[(p-1)! t x_{p-1}^p - d^{p-2}x_{p-1}/dt^{p-2} - d^{p-2}c(t)/d^{p-2}t\right] = 0,$$

so there exists $x_{p-2} \in \mathbf{F}_q[[t]]$ such that

$$d^{p-2}c(t)/dt^{p-2} = (p-2)! x_{p-2}^p + (p-1)! x_{p-1}^p - d^{p-2}x_{p-1}/dt^{p-2}.$$

By repeating this argument $p-2$ times, we can find $x_0, \ldots, x_{p-1} \in \mathbf{F}_q[[t]]$ such that $c(t) = P(x_0, \ldots, x_{p-1})$, and (2) is proved.

Finally, we claim that

(4) *for an element* $c \in \mathbf{F}_q$, $ct^{-1} \in P(k_v \times \cdots \times k_v)$ *if and only if* $c = u^p - u$, *for some* $u \in \mathbf{F}_q$.

In fact, if $ct^{-1} = P(a_0, \ldots, a_{p-1}), a_0, \ldots, a_{p-1} \in k_v$, then again, by differentiating with respect to t this equality $(p-1)$ times , we get

$$ct^{-p} = a_{p-1}^p + d^{p-1}a_{p-1}/dt^{p-1}. \tag{5}$$

It suffices to consider the case $c \neq 0$. In this case, $a_{p-1} \neq 0$, and we can write $a_{p-1} = t^l u$, where $l \in \mathbf{Z}, u \in k_v$, $v_t(u) = 0$, and v_t denotes the valuation corresponding to t. If $l \geq 0$ then

$$v_t(a_{p-1}^p + d^{p-1}a_{p-1}/dt^{p-1}) \geq 0.$$

We note that for any $a \in k_v$ then $v_t(da/dt) \geq v_t(a) - 1$, so

$$v_t(d^{p-1}a_{p-1}/dt^{p-1}) \geq l - (p-1).$$

If $l \leq -2$ then

$$v_t(d^{p-1}a_{p-1}/dt^{p-1}) \geq l - (p-1) > pl = v_t(a_{p-1}^p),$$

hence

$$v_t(a_{p-1}^p + d^{p-1}a_{p-1}/dt^{p-1}) = pl < -p = v_t(ct^{-p}).$$

So, by comparing both sides of (5) we find that $l = -1$. By using Leibnitz's Formula and Wilson's Theorem again, we obtain

$$ct^{-p} = t^{-p}u^p - t^{-p}u + \sum_{i=0}^{p-2} C_{p-1}^i (-1)^i i! t^{-(i+1)} d^{p-1-i}u/dt^{p-1-i}. \tag{6}$$

Let $u = u_0 + tu_1$, $u_0 \in \mathbf{F}_q, u_1 \in \mathbf{F}_q[[t]]$. By comparing the coefficients of t^{-p} in both sides of (6), we get $c = u_0^p - u_0$. Conversely, if $c = u^p - u$, for some $u \in \mathbf{F}_q$, then $ct^{-1} = P(0, \ldots, 0, ut^{-1})$.

From (1), (2), (4) we have $|\mathrm{H}^1(k_v, G)| = |\ker \varphi|$, where φ is the homomorphism: $(\mathbf{F}_q, +) \to (\mathbf{F}_q, +), u \mapsto u^p - u$. It is clear that $|\ker \varphi| = |\mathbf{F}_p| = p$. Hence $|\mathrm{H}^1(k_v, G)| = p$.

b) By Lemma 4.1, we have $[k^{1/p} : k] = p$. By [Oe], Ch. VI, Sec.5, G is isomorphic to the quotient of the Weil restriction $\prod_{k^{1/p}/k} \mathbf{G}_m$ by $\mathbf{G}_m$, and from [Oe, Chap. VI, Sec. 5.4, Proposition 2], it follows that G has Tamagawa number $\tau_G = p$. Then, by using the Hasse principle for the Brauer group of

global fields (see, e. g. [We]) one checks that $Ш(G) = 1$.
Now, assume that $\mathrm{H}^1(k, G)$ is finite. Then $\mathrm{H}^1(k_v, G)$ is trivial for almost all v, since

$$\mathrm{H}^1(k, G) \to \prod_{v \in F} \mathrm{H}^1(k_v, G)$$

is surjective for any finite set F of discrete valuations ([TT]). Let

$$\gamma : \mathrm{H}^1(k, G) \to \prod_{v} \mathrm{H}^1(k_v, G))$$

be the localization map and let S be the finite set of v such that $\mathrm{H}^1(k_v, G) \neq 0$. The map $\mathrm{H}^1(k, G) \to \prod_{v} \mathrm{H}^1(k_v, G))$ is thus surjective, so by [Oe], Ch. IV, Corollaire 3.4, we have the following formula for the Tamagawa number τ_G of G :

$$\tau_G = \frac{|Ш(G)|}{|\mathrm{Coker}\ \gamma|} = \frac{1}{|\mathrm{Coker}\ \gamma|} \leq 1.$$

This is contradicting to the fact that $\tau_G = p$. Therefore $\mathrm{H}^1(k, G)$ is infinite.

c) Using the same argument as in part a), we get $|\mathrm{H}^1(k_v, G)| = |\ker \varphi|$, where φ is the homomorphism: $(\mathbf{F}_q, +) \to (\mathbf{F}_q, +), u \mapsto u^p + u$. Note that $\ker \varphi$ is a normal subgroup of $\mathbf{F}_q$ and has at most p elements, then $|\ker \varphi| = 1$ or p. If $|\ker \varphi| = p$ then the polynomial $X^{p-1} + 1$ can be split into linear factors over $\mathbf{F}_q[X]$ and $\mathbf{F}_q$ contains a $(p-1)^{th}$-root of -1. Conversely, if $\mathbf{F}_q$ contains a $(p-1)^{th}$-root α of -1 then $\alpha, 2\alpha, \ldots, (p-1)\alpha$ are all roots of $X^{p-1}+1$ and $|\ker \varphi| = p$. It is clear that $\mathbf{F}_q$ contains a $(p-1)^{th}$-root of -1 if and only if $\mathbf{F}_q$ contains a primitive $2(p-1)$-root of unity, $\zeta_{2(p-1)}$. Since $\mathbf{F}_{p^n}$ is the splitting field of $X^{p^n} - X = 0$ over $\mathbf{F}_p$, $\mathbf{F}_{p^n}$ contains $\zeta_{2(p-1)}$ if and only if $\zeta_{2(p-1)}^{p^n-1} = 1$, i.e., $2(p-1)$ divides $p^n - 1$, that is, if and only if n is even. ∎

Further, we give another example of a wound unipotent group defined over $\mathbf{F}_p(t)$, which , when passing to $\mathbf{F}_q((t))$, $q = p^n$, has trivial Galois cohomology group, for any n (compare with Proposition 4.3, c)).

4.4. Proposition. *Let $k_v = \mathbf{F}_q((t))$, where $q = 3^n$, and let G be the $\mathbf{F}_p(t)$-subgroup of $\mathbf{G}_a^3$ defined as follows*

$$G = \{(x_1, x_2, x_3) | x_1^3 + t x_2^3 + t^{-1} x_3^3 + x_3 = 0\}.$$

Then $\mathrm{H}^1(k_v, G) = 0$.

Proof. Let $P(x_1, x_2, x_3) = x_1^3 + tx_2^3 + t^{-1}x_3 + x_3$. By an analogous argument as in previous proposition, we have $\mathrm{H}^1(k_v, G) \simeq k_v/P(k_v \times k_v \times k_v)$. Hence, to prove the triviality of $\mathrm{H}^1(k_v, G)$, we need only prove the following:

(1) $\mathbf{F}_q[[t]] \subset P(\mathbf{F}_q[[t]] \times \mathbf{F}_q[[t]] \times \mathbf{F}_q[[t]])$, *i.e.* $\sum_{i\geq 0} c_i t^i \in P(\mathbf{F}_q[[t]] \times \mathbf{F}_q[[t]] \times \mathbf{F}_q[[t]])$, *for all* $c_i \in \mathbf{F}_q$,

(2) $ct^{-i} \in P(k_v \times k_v \times k_v)$, *for all* $c \in \mathbf{F}_q, i \geq 1$.

Now, we prove (1). By differentiating both sides of the following equation with respect to t twice

$$\sum_{i\geq 0} c_i t^i = x_1^3 + tx_2^3 + t^{-1}x_3^3 + x_3,$$

we get

$$(\star\star) \qquad \sum_{i\geq 0} 2c_{3i+2}t^{3i} = 2t^{-3}x_3^3 + d^2x_3/dt^2.$$

By writing $x_3 = \sum_{i\geq 0} a_i t^i, a_i \in \mathbf{F}_q$ we have

$$2t^{-3}x_3^3 + d^2x_3/dt^2 = 2a_0^3 t^{-3} + \sum_{i\geq 0}(2a_{i+1}^3 + 2a_{3i+2})t^{3i}.$$

Comparing coefficients with the same power of t in $(\star\star)$ we get

$$a_0 = 0, \;\; 2a_{i+1}^3 + 2a_{3i+2} = 2c_{3i+2}, \; \forall i \geq 0.$$

By setting $a_{3i} = a_{3i+1} = 0, a_{3i+2} = -a_{i+1}^3 + c_{3i+2}, \forall i \geq 0$, we get a solution for $(\star\star)$. Since

$$\frac{d}{dt}\left[\sum_{i\geq 0}(c_{3i+1}t^{3i} + 2c_{3i+2}t^{3i+1}) - (-t^{-2}x_3^3 + dx_3/dt)\right] = 0,$$

there exists $x_2 \in \mathbf{F}_q[[t]]$ such that

$$\sum_{i\geq 0}(c_{3i+1}t^{3i} + 2c_{3i+2}t^{3i+1}) = x_2^3 - t^{-2}x_3^3 + dx_3/dt.$$

Using this argument again, we have $\sum_{i\geq 0} c_i t^i = P(x_1, x_2, x_3)$, for some $x_1, x_2, x_3 \in \mathbf{F}_q[[t]]$.

Finally, we prove (2) by induction on i. Namely, given any $c \in \mathbf{F}_q$, then $c = \beta^3, \beta = \alpha^3, \alpha, \beta \in \mathbf{F}_q$. We have $ct^{-1} = P(-\alpha, 0, \beta)$, and $ct^{-2} = P(0, \beta t^{-1}, 0)$. So (2) is true for $i = 1, 2$. And it is easy to check that $ct^{-3i} = P(\beta t^{-i}, 0, 0)$, $ct^{-3i+1} = P(0, \beta t^{-i}, 0)$, and $ct^{-3i+2} = P(a, b, c+\beta t^{-i+1})$, where $a, b, c \in K$, satisfy $-\beta t^{-i} = P(a, b, c)$ (the existence of a, b, c are ensured by the induction hypothesis). ∎

4.5. Now we give a sufficient condition for the Galois cohomology groups of unipotent commutative groups over non-perfect field to be infinite. Then, using this, we prove that the only connected smooth unipotent group of dimension 1 with finite Galois cohomology group over global field is $\mathbf{G}_a$. Before stating and proving this condition, we need the following lemma. Recall that if P is a p-polynomial in r variables $T_1, ..., T_r$, with

$$P = \sum_{1\leq i\leq r} \sum_{0\leq j\leq m_i} c_{ij} T_i^{p^j}, \quad \text{where } \ c_{im_i} \neq 0, \forall i,$$

then the principal part P_{princ} of P is defined by

$$P_{princ} = \sum_{1\leq i\leq r} c_{im_i} T_i^{p^{m_i}}.$$

Lemma. *Let k be a non-perfect field of characteristic p, v a non-trivial discrete valuation of k. Let P be a separable p-polynomial in r variables with coefficients in k. Let $P_{princ} = \sum_{i=1}^{r} c_i T_i^{p^{m_i}}$ be the principal part of P. Assume that for all $(a_1, \ldots, a_r) \in k^r$, $v(c_i) + p^{m_i} v(a_i)$ are all distinct whenever they are finite. Then there exists a constant C_0 depending only on P, such that if $a = P(a_1, \ldots, a_r)$ and $v(a) \leq C_0$ then $v(a) = v(c_i) + p^{m_i} v(a_i)$, for some i.*

Proof. We process by induction on r. By assumption, P is a non-zero p-polynomial. First let $r = 1$, $P(T) = c_0 T + \cdots + c_{m-1} T^{p^{m-1}} + c_m T^{p^m}$. We set

$$A = \inf_{i,j} \{\frac{v(c_i) - v(c_j)}{p^j - p^i} \mid 0 \leq i, j \leq m, i \neq j\},$$

$$B = \inf \{Ap^i + v(c_i) \mid 0 \leq i \leq m\} - 1,$$

and pick any C_0 with $C_0 < B$. Now assume that $a = P(a_1)$ such that $v(a) = v(P(a_1) \leq C_0$ $(a_1 \in k)$. Let i_0 be such that

$$v(c_{i_0} a_1^{p^{i_0}}) = \inf \{v(c_i a_1^{p^i}) \mid 0 \leq i \leq m\}.$$

Then we have $C_0 \geq v(a) = v(P(a_1)) \geq v(c_{i_0} a_1^{p^{i_0}}) = v(c_{i_0}) + p^{i_0} v(a_1)$. Hence

$$(C_0 - v(c_{i_0}))/p^{i_0} \geq v(a_1).$$

By the choice of C_0, B, and A we have

$$v(a_1) < (B - v(c_{i_0}))/p^{i_0} < (Ap^{i_0} + v(c_{i_0}) - v(c_{i_0}))/p^{i_0} = A.$$

Hence by the definition of A

$$v(a_1) < \frac{v(c_i) - v(c_m)}{p^m - p^i}, \ \ \forall i < m,$$

or, equivalently,

$$v(c_i a_1^{p^i}) = v(c_i) + p^i v(a_1) > v(c_m) + p^m v(a_1) = v(c_m a_1^{p^m}), \ \forall i < r.$$

Therefore $v(a) = v(c_m) + p^m v(a_1)$ as required.

Now we assume $r > 1$ and that the assertion of the lemma holds true for all integers less than r. By induction hypothesis, for any l with $1 \leq l < r$, there exist constants B_l satisfying the lemma for the case $r = l$. Any monomial of $P(T_1, \ldots, T_r) - P_{princ}(T_1, \ldots, T_r)$ is of the form $\lambda T_j^{p^{m_j - s}}$, $\lambda \in k^*, 1 \leq j \leq r, s \geq 1$, and for such a monomial, we set

$$a_{\lambda,s,j} = \frac{v(\lambda) - v(c_j)}{p^{m_j} - p^{m_j - s}},$$

and set

$$C_3 = \left[\inf_{\lambda,j,s,i} \{(v(\lambda) + p^{m_j - s} a_{\lambda,j,s} - v(c_i)) p^{-m_i}\} \right] - 1.$$

Let

$$C_2 = \left[\inf_{1 \leq i,j \leq r} \{(v(c_i) + p^{m_i} C_3 - v(c_j)) p^{-m_j}\} \right],$$

$$C_1 = \inf_{i,j} \{v(c_{ij}) + p^{m_{ij}} C_2\},$$

$$C_0 = \inf \{C_1, B_1, \ldots, B_{r-1}\}.$$

Assume that $a = P(a_1, \ldots, a_r), a_i \in k$ and $v(a) \leq C_0$. If there exists i such that $a_i = 0$ then $|\{i \mid a_i \neq 0\}| < r$ and instead of P we may consider the polynomial $\tilde{P} = P(T_1, \ldots, T_{i-1}, 0, T_{i+1}, \ldots, T_r)$ in $r-1$ variables and use the induction hypothesis. So, we assume that $a_i \neq 0$ for all i. Let

$$i_0 = \inf_{1 \leq i \leq r} \{i \mid v(a_i) \leq v(a_j), \text{for all } j, 1 \leq j \leq r\}.$$

Then

$$v(a) = v(P(a_1, \ldots, a_r)) \geq \inf\{v(c_{ij} a_i^{p^{m_{ij}}})\} \geq \inf\{v(c_{ij}) + p^{m_{ij}} v(a_{i_0})\}.$$

By assumptions $v(a) \leq C_0 \leq C_1$, so we have $v(a_{i_0}) \leq C_2$ by definition of C_1. Since $v(c_i) + p^{m_i} v(a_i)$ are pairwise distinct, there exists unique i_1 such that

$$v(c_{i_1}) + p^{m_{i_1}} v(a_{i_1}) = \inf_{1 \leq j \leq r} \{v(c_j) + p^{m_j} v(a_j)\}.$$

Since

$$v(c_{i_1}) + p^{m_{i_1}} v(a_{i_1}) \leq v(c_{i_0}) + p^{m_{i_0}} v(a_{i_0}) \leq v(c_{i_0}) + p^{m_{i_0}} C_2,$$

we have $v(a_{i_1}) \leq C_3$, since otherwise, we would have

$$v(c_{i_1}) + p^{m_{i_1}} v(a_{i_1}) > v(c_{i_1}) + p^{m_{i_1}} C_3 \geq v(c_{i_0}) + p^{m_{i_0}} C_2,$$

which contradicts the above inequalities. Now, we show that

$$v(P(a_1, \ldots, a_r)) = v(c_{i_1}) + p^{m_{i_1}} v(a_{i_1}).$$

This follows from the following two facts:
(i) For any monomial $\lambda T_j^{p^{m_j - s}}$ of $P(T_1, \ldots, T_r) - P_{princ}(T_1, \ldots, T_r)$, appearing in $P(T_1, ..., T_r)$, $\lambda \in k, 1 \leq j \leq r, s \geq 1$, if $v(a_j) < a_{\lambda,j,s}$ then by the definition of $a_{\lambda,s,j}$ and i_1, we have

$$v(\lambda a_j^{p^{m_j - s}}) = v(\lambda) + p^{m_j - s} v(a_j) > v(c_j) + p^{m_j} v(a_j) \geq v(c_{i_1}) + p^{m_{i_1}} v(a_{i_1}).$$

Also, if $v(a_j) \geq a_{\lambda,j,s}$ then again by the definition of $a_{\lambda,s,j}$ and C_3, we have

$$v(\lambda a_j^{p^{m_j - s}}) \geq v(\lambda) + p^{m_j - s} a_{\lambda,j,s} > v(c_{i_1}) + p^{m_{i_1}} C_3 \geq v(c_{i_1}) + p^{m_{i_1}} v(a_{i_1}),$$

since $v(a_{i_1}) \leq C_3$. Thus, we have for all j

$$v(\lambda a_j^{p^{m_j - s}}) \geq v(c_{i_1}) + p^{m_{i_1}} v(a_{i_1}).$$

Hence

$$v(P(a_1,...,a_r) - P_{princ}(a_1,...,a_r)) \geq v(c_{i_1}) + p^{m_{i_1}} v(a_{i_1}).$$

(ii) For $j \neq i_1$, by the uniqueness of i_1, we have

$$v(c_j a_j^{p^{m_j}}) > v(c_{i_1}) + p^{m_{i_1}} v(a_{i_1}),$$

so

$$v(P_{princ}(a_1,...,a_r)) = v(c_{i_1} a_{i_1}^{p^{m_{i_1}}} + \sum_{j \neq i_1} c_j a_j^{p^{m_j}}) > v(c_{i_1} a_{i_1}^{p^{m_{i_1}}}).$$

Now from above it follows that

$$\begin{aligned} v(a) &= v(P(a_1,...,a_r)) \\ &= v(P_{princ}(a_1,...,a_r) + (P(a_1,...,a_r) - P_{princ}(a_1,...,a_r)) \\ &= v((c_{i_1} a_{i_1}^{p^{m_{i_1}}} + \sum_{j \neq i_1} c_j a_j^{p^{m_j}}) + (P(a_1,...,a_r) - P_{princ}(a_1,...,a_r))) \\ &= v(c_{i_1} a_{i_1}^{p^{m_{i_1}}}) = v(c_{i_1}) + p^{m_{i_1}} v(a_{i_1}). \end{aligned}$$

The proof of the lemma is completed. ∎

4.6. Proposition. *Let k be a non-perfect field of characteristic p, v a non-trivial discrete valuation of k. Let G be a commutative unipotent group defined by a separable p-polynomial P in r variables, with $P_{princ} = \sum_{i=1}^{r} c_i T_i^{p^{m_i}}$, $c_i \in k^*$. Let $m = \min\{m_1, \ldots, m_r\}$ and assume that $v(c_1), \ldots, v(c_r)$ are all distinct modulo p^m and $r < p^m$. Then $\mathrm{H}^1(k, G)$ is infinite.*

Proof. Since $v(c_1), \ldots, v(c_r)$ are all distinct modulo p^m, then for any tuple $(a_1, \ldots, a_r) \in k^{*r}$, the values $v(c_i) + p^{m_i} v(a_i)$, $1 \leq i \leq r$, are always pairwise distinct. Then all assumptions in the above lemma are satisfied, so there exists C_0 as in the lemma. Since $r < p^m$ then there exists l in $\{0, \ldots, p^m - 1\}$ such that $v(c_i) \not\equiv l (\mathrm{mod}\, p^m)$, for all $i \in \{1, .., r\}$. We claim that for all a with $v(a) \leq C_0$, and $v(a) \equiv l \pmod{p^m}$, then a is not in $P(k^r)$. For, assume the contrary that $a = P(a_1, \ldots, a_r), a_i \in k$. By the lemma above, there is i such that $v(a) = v(c_i) + p^{m_i} v(a_i)$. But

this is contradicting to the fact that $v(c_i) \not\equiv l \pmod p$, hence the claim follows. We can choose a sequence $\{b_n\}_n$, $b_n \in k$ for all $n \geq 1$, such that $C_0 > v(b_1) > v(b_2) > \cdots > v(b_n) \equiv l \pmod{p^m}$, for all n. Then $v(b_n - b_{n+m}) = v(b_{n+m}) \equiv l \pmod{p^m}$, for all $m, n \geq 1$. Therefore by the claim above, for all $m, n \geq 1$ then $b_n - b_{n+m} \notin P(k^r)$, so all b_n are distinct in $k/P(k^r)$. Therefore $\mathrm{H}^1(k, G)$ is infinite as required. ∎

Obvious examples (cf. 4.2, 4.3) show that one cannot relax the condition "$r < p^m$" to "$r \leq p^m$", or relax the condition that the valuations $v(c_i)$ are all distinct (mod. p^m). As application of the above result, we show that the flat cohomology in dimension 1 of one-dimensional non-split unipotent group over non-perfect fields are infinite in general. First we consider the one-dimensional flat cohomology of elementary finite unipotent group schemes. In the simplest case of $\mathbf{Z}/p\mathbf{Z}$, the finiteness result dated back to Shatz [Sh].

4.7. Proposition. *Let k be a non-perfect field of characteristic $p > 0$.*
a) Denote by α_n the affine k-group scheme corresponding to $k[T]/(T^n)$. For any $r \geq 1$, let G be a k-form of α_{p^r} or $(\mathbf{F}_p)^r$. Then $\mathrm{H}^1_{fl}(k, G)$ is infinite.
b) Let G be a non-trivial unipotent k-group scheme of dimension 0. Then $\mathrm{H}^1_{fl}(k, G)$ is infinite.

Proof. *a*) In our situation, there exists a descending central series for G

$$G = G_0 > G_1 > \cdots > G_{n-1} > G_n = \{0\}$$

with successive quotients G_i/G_{i+1} isomorphic to a k-form of $(\alpha_p)^r$ or $(\mathbf{F}_p)^r$ (see [DG], or Raynaud [SGA 3, Exposé XVII]). By making use of the fact that all groups G_i involved are commutative and $\mathrm{H}^2_{fl}(k, G_i) = 0$ (see e. g. [DG], Chap. III, §5, Corol. 5.8 , and [Se1], Chap. II, §2), it is clear that it suffices to prove the proposition in the case $r = 1$. We can find and fix once for all a non-trivial discrete valuation v of k. It is well known (see e.g. [DG], Chap. III, Raynaud [SGA 3], Exposé XVII), that α_p has no non-trivial k-forms and $\mathrm{H}^1_{fl}(k, \alpha_p) \simeq k^+/k^{+p}$. For any element a in k^* with $v(a) \not\equiv 0 \pmod p$, it is clear that a is not in k^p. We may construct an infinite sequence $\{a_i\}$, $a_i \in k$, such that $v(a_1) < v(a_2) < \cdots < v(a_n)$ and $v(a_n) \not\equiv 0 \pmod p$ for all n. Then obviously $a_i \pmod{k^p}$ are pairwise distinct, hence the abelian group k^+/k^{+p} (i.e. $\mathrm{H}^1_{fl}(k, \alpha_p)$) is infinite.

Now let G be a k-form of $(\mathbf{F}_p)^r$. Then we know that G can be embedded as a closed k-subgroup of exponent p into $\mathbf{G}_a$. The exact sequence

$$0 \to G \to \mathbf{G}_a \xrightarrow{f} \mathbf{G}_a \to 0$$

allows us to consider G as the kernel (hence also as zero set) of a separable p-polynomial $f = f(T) \in k[T]$. Since G has p^r elements, we have $\deg(f) \geq p^r$. Hence $f(T) = b_0T + \cdots + b_sT^{p^s}, b_s \neq 0, s \geq r$. Up to a k-isomorphism, we may scale off b_s, so we may assume that $b_s = 1$. Then $\mathrm{H}^1(k, G) \simeq k/f(k)$, where $f(x) = b_0x + \cdots + b_{s-1}x^{p^{s-1}} + x^{p^s}$ Now, consider the constant C_0 depending only on the p-polynomial $f(T)$ (with the only leading coefficient $c = 1$) as in Lemma 4.5. For z in k such that $v(z) < C_0$ and $v(z) \not\equiv 0 \pmod p$, we see, according to this lemma, that z is not in $f(T)$. Again as above we may choose an infinite sequence $\{a_i\}$ of elements from k such that $a_i \notin f(k)$, $C_0 > v(a_1) > v(a_2) > \cdots > v(a_i) > \cdots$ for all i, and from this we conclude that $\mathrm{H}^1(k, G)$ is infinite.

b) The proof is again by "dévisage". First we assume that G is commutative. By Raynaud [SGA 3, Exposé XVII], there is a composition series for G

$$G = G_0 > G_1 > \cdots > G_r > G_{r+1} > \cdots > G_m = \{0\},$$

where each factor G_i/G_{i+1} is a k-form of $(\mathbf{F}_p)^r$ (resp. of $(\alpha_p)^r$) for $0 \leq i \leq r-1$ (resp. for $r \leq m-1$). The rest follows from the proof of part *a*).

Now assume that G is not necessarily commutative and let $C(G)$ denote the center of G. We use induction on the length $s = s(G)$ of ascending central series of G, which is finite since G is nilpotent. If $s = 1$, then G is commutative and we are back to the above case. Let $s(G) = m > 1$ and assume that the assertion holds for all $1 \leq s < m$. We have $s(G/C(G)) < s(G)$. Since $G/C(G)) \neq \{1\}$ and has dimension 0, and since $\mathrm{H}^2_{fl}(k, C(G)) = 0$, the induction hypothesis implies that $\mathrm{H}^1_{fl}(k, G/C(G))$ (and hence also $\mathrm{H}^1_{fl}(k, G)$) is infinite. ∎

For unipotent groups of positive dimension we have the following result.

4.8. Theorem. *Let k be a non-perfect field of characteristic p. Let G be a non-trivial (not necessarily smooth) commutative unipotent k-group scheme of dimension ≤ 1, the connected component G° of which is not k-isomorphic*

to an extension of $\mathbf{G}_a$ *by an infinitesimal k-group scheme. Assume in addition that if* $p = 2$ *then* G° *is neither k-isomorphic to an extension of* $\mathbf{G}_a$*, nor of the subgroup defined as in Proposition 4.2, b), by an infinitesimal group scheme. Then the flat cohomology* $\mathrm{H}^1_{fl}(k, G)$ *is infinite. In particular, for any global field k of positive characteristic and for any non-trivial commutative k-unipotent group scheme G of dimension* ≤ 1 *with* G° *not k-isomorphic to an extension of* $\mathbf{G}_a$*, by an infinitesimal k-group, the cohomology set* $\mathrm{H}^1_{fl}(k, G)$ *is infinite.*

Proof. I) First, we assume that G is commutative, smooth (i.e. absolutely reduced) and connected.

If G has dimension 0, the assertion follows from Proposition 4.7.

Assume that dim (G) =1. Then by [Ru], G is a k-form of $\mathbf{G}_a$, and G is k-isomorphic to a k-subgroup of $\mathbf{G}_a \times \mathbf{G}_a$ given by

$$\{(x, y)|y^{p^n} = x + a_1x^p + \cdots + a_nx^{p^m}\},$$

where $a_1, \ldots, a_m$ are elements of k not all in k^p. It is well known (see e. g. [Mi1]) that if G is reduced then $\mathrm{H}^1_{fl}(k, G) \simeq \mathrm{H}^1(k, G)$. Let $P_n(x, y) = x + a_1x^p + \cdots + a_mx^{p^m} - y^{p^n}$, $a_m \neq 0$, then by an analogous argument as in Proposition 4.2 we have $\mathrm{H}^1(k, G) \simeq k/P_n(k^2)$.

a) We consider the case $p > 2$. Evidently, $P_n(k^2) \subset P(k^2)$, where $P := P_1$. Therefore, we need only consider the case $n = 1$. Let v be a non-trivial discrete valuation with a prime element π, k_v the completion of k respect to v. Then we know (cf. [TT]) that the localization map $\mathrm{H}^1(k, G) \to \mathrm{H}^1(k_v, G)$ is surjective. Therefore, it suffices to consider the local case, i.e, to show that $\mathrm{H}^1(k_v, G)$ is infinite. In the sequel we identify k_v with the field $k(v)[[\pi]]$. If $a_m \in k_v^p$ then by changing the variables

$$y' = y - \alpha x^{p^{m-1}},\ x' = x,$$

where $a_m = \alpha^p$, $\alpha \in k_v$, G is isomorphic to the group given by

$$\{(x', y')|y'^p = x' + a_1x'^p + \cdots + a_{m-1}x'^{p^{m-1}}\}.$$

Hence, by repeating this argument (if necessary), we may assume that a_m is not in k_v^p, with $m \geq 1$, since by assumption, $G \not\simeq \mathbf{G}_a$. Assume that $v(a_m) \equiv 0 \pmod p$. We recall the following result from [Ru], Proposition

2.3. Denote by F the Frobenius morphism, $A = k[F]$ the (non-commutative) ring of polynomials in F subject to the relation $Fa = a^p F$, for all $a \in k$. Then $A \simeq \mathrm{End}_k(\mathbf{G}_a, \mathbf{G}_a)$, the ring of k-endomorphisms of G_a. Every k-form G of the k-group $\mathbf{G}_a$ is then defined by the tuple (F^n, τ), where $\tau = a_0 + a_1 F + \cdots + a_m F^m \in A, a_0 \neq 0$ (a separable endomorphism), and it is k-isomorphic to the k-subgroup of $\mathbf{G}_a \times \mathbf{G}_a$ defined by the equation

$$y^{p^n} = a_0 + a_1 x^p + \cdots + a_m x^{p^m}.$$

By [Ru, Prop. 2.3], the two k-forms (F^n, τ), (F^{n_1}, τ_1), with $n_1 \leq n$, $\tau_1 = c_0 + c_1 F + \cdots + c_{m_1} F^{m_1}$, are k-isomorphic if and only if there exist a separable endomorphism $\rho = b_0 + b_1 F + \cdots + b_r F^r \in A$, $\sigma \in A$, and $c \in k^*$ such that

$$(\sum_{0 \leq j \leq m_1} c_j^{p^{n-n_1}} F^j)c = (\sum_i b_i^{p^n} F^i)\tau + F^n \sigma.$$

Using this we may choose a k-form of $\mathbf{G}_a$ defined by the equation $y^p = a'_0 + a'_1 x^p + \cdots + a'_n x^{p^n}$, which is still k-isomorphic to G, such that $v(a'_n) \not\equiv 0 \pmod{p}$. Now, all conditions in Proposition 4.6 are satisfied. Namely, we have $P_{princ} = a'_m x'^{p^m} - y'^p$, $r = 2 < p = p^{\inf\{1,m\}}$, and $v(a'_m), v(-1)$ are distinct modulo p. Therefore, by Proposition 4.6, $\mathrm{H}^1(k_v, G)$ is infinite.

b) Now we consider the case when $p = 2$.
*b*1) Assume first that G is not isomorphic to the subgroup of $\mathbf{G}_a \times \mathbf{G}_a$ defined by the equation

$$\{(x, y) | y^{2^n} = x + a_1 x^2\},$$

where $n \geq 2, a_1 \notin k^2$. By the same argument as in the case $p > 2$, it suffices to consider the local case, i.e., over k_v, $n = 1$, $m \geq 2$, and by applying [Ru, Prop. 2.3] if necessary,, we may assume that $v(a_m) \equiv 1 \pmod{2}$. But then $v(w^2) = 2v(w)$ and $v(a_m) + 2^m v(u)$ are always distinct whenever $(u, w) \in k^{*2}$. We choose an odd number $l \pmod 4$ such that $v(a_m) \not\equiv l \pmod 4$. By Lemma 4.5, there exists a constant C_0 such that if $a = P(u, w)$, $v(a) \leq C_0$ then $v(a) = v(w^2)$ or $v(a) = v(a_m) + 2^m v(u)$. We claim that if $a \in k_v$ satisfies the conditions $v(a) \equiv l \pmod 4$ and $v(a) \leq C_0$ then $a \notin P(k^2)$. In fact, assume that $a = P(u, w), u, w \in k$. Since $v(a) \leq C_0$, $v(a) = v(w^2)$ or $v(a_m) + 2^m v(u)$. But this contradicts to the fact that $v(a) \equiv l \pmod 4$. We conclude as in the proof of Proposition 4.6 that $\mathrm{H}^1(k, G)$ is infinite.

*b*2) We now assume that $p = 2$ and G is isomorphic to a subgroup of the

above Russel's form. It is sufficient to treat the case $n = 1, m = 2$. By making use of [Ru, Prop. 2.3], we may again assume that $v(a_1) \equiv 1 \pmod 2$. Then $v(a_1) \equiv 1 \text{ or } 3 \pmod 4$. So, $v(w^4)$ and $v(a_1) + 2v(u)$ are always distinct whenever $(u, w) \in k^{*2}$. We use an analogous argument as in previous case and we see that $\mathrm{H}^1(k, G)$ is infinite.

II) We now assume that G is commutative, connected and non-smooth. Let α_{p^r} be the k-group scheme represented by Spec $k[T]/(T^{p^r})$. If dim $G = 0$, then G is a k-form of α_{p^r} for some r, thus isomorphic to the latter (here we used the fact that r-multiple extension of α_p by itself is isomorphic to α_{p^r} (see Raynaud [SGA 3, Exp. XVII]), and by Proposition 4.7, it has infinite flat cohomology.

Now we assume that dim $G = 1$. Denote by F the Frobenius morphism on G, $G^{(p)}$ the k-group scheme obtained from G via the base change $k \to k^p$. For any natural number n, by considering F^n we obtain $G^{(p^n)}$ and we denote ${}_{F^n}G := \mathrm{Ker}\,(F^n) : G \to G^{(p^n)}$. Then it is well-known (see Gabriel [SGA 3, Exp. VI_A]) that there is a natural number n_0 such that $G/_{F^n}G$ is smooth for all $n \geq n_0$. Let r be the smallest such a number. Then $r \geq 1$ since G is non-smooth, and we have the following composition series of characteristic subgroups of G

$$G \geq G^\circ \geq {}_{F^r}G \geq \cdots \geq {}_{F}G \geq (0).$$

Here G° denotes the connected component of G, and each factor ${}_{F^{s+1}}G/_{F^s}G$, $1 \leq s \leq r-1$ is a radicial (infinitesimal) k-subgroup scheme of height 1 (loc.cit). Therefore we have an exact sequence

$$(\star) \qquad 0 \to \alpha_{p^r} \to G \to G_{red} \to 0,$$

where G_{red} is reduced. Then G_{red} is a k-form of $\mathbf{G}_a$. From the exact sequence $(\star)$, we derive the exact sequence of flat cohomology

$$\mathrm{H}^1_{fl}(k, G) \xrightarrow{f} \mathrm{H}^1_{fl}(k, G_{red}) \to \mathrm{H}^2_{fl}(k, \alpha_{p^r}).$$

By [DG], Chap. III, §5, Corol. 5.8, $\mathrm{H}^2_{fl}(k, \alpha_{p^r}) = 0$, so f is surjective. By assumption, $G_{red} \not\simeq \mathbf{G}_a$, and if $p = 2$, G_{red} is not k-isomorphic to the group defined in Proposition 4.2, b), also. So by previous part, $\mathrm{H}^1_{fl}(k, G_{red}) \simeq \mathrm{H}^1(k, G_{red})$ is infinite, and it follows that the same is true for $\mathrm{H}^1_{fl}(k, G)$.

III) Next we assume that G is commutative, but not connected (and not necessarily smooth) so $G/G^0 \neq \{1\}$ and consider the following exact sequence

$$1 \to G^0 \to G \to G/G^0 \to 1,$$

where G^0 denotes the connected component of G. Then we have $\dim(G) = \dim(G^0) = 1$. Also, since G is commutative we have the following exact sequence of flat cohomology

$$\mathrm{H}^1_{fl}(k, G^\circ) \to \mathrm{H}^1_{fl}(k, G) \xrightarrow{\beta} \mathrm{H}^1_{fl}(k, G/G^\circ) \to \mathrm{H}^2_{fl}(k, G^\circ).$$

Since G° is a commutative unipotent group scheme, from the exact sequence (like $(*)$ above)

$$0 \to \alpha_{p^r} \to G^\circ \to G^\circ_{red} \to 0,$$

and from the triviality of H^2_{fl} for α_{p^r} and G°_{red}, it follows that $\mathrm{H}^2_{fl}(k, G^\circ) = 0$, so β is surjective. It then suffices to show that $\mathrm{H}^1_{fl}(k, G/G^0)$ is infinite. It is known that $H := G/G^0$ is a finite étale unipotent k-group scheme, hence it has a composition series

$$H = H_0 > H_1 > \cdots > H_t = \{0\}$$

with successive factors H_i/H_{i+1} isomorphic to a k-form of $(\mathbf{F}_p)^r$ for some r. By Proposition 4.7, $\mathrm{H}^1_{fl}(k, H)$ is infinite as well, hence so is $\mathrm{H}^1_{fl}(k, G)$.

IV) Now assume that k is a global function field of characteristic p. We refer to Proposition 4.2, *b*), Proposition 4.7, and the previous parts for the rest of the proof. ∎

(Notice that, by using [DG], III, Section 6, one can show that the condition that G° not to be an extension of $\mathbf{G}_a$ by an infinitesimal unipotent k-group can be relaxed to the condition that $G^\circ \not\simeq \mathbf{G}_a$, which is not essential.)

4.9. Corollary. *Let k be a non-perfect field of characteristic $p > 0$. Then, for all r, there exists a k-form of $\mathbf{G}_a^r$ such that $\mathrm{H}^1(k, G)$ is infinite.*

Proof. It is well known that for any non-perfect field k, there are many discrete valuations of k. For example, if p =char.k, t a transcendental element of k over $\mathbf{F}_q$, then one may associate a nontrivial discrete valuation v_t associated to t (see e.g. [Bou], Chap. VI). Then by using Proposition 4.6, we may choose a k-form G of $\mathbf{G}_a^r$ with infinite $\mathrm{H}^1(k, G)$. ∎

It is quite possible that for any k-split unipotent group G over non-perfect field k, there is a k-form G' of G which has infinite cohomology. In [Ro2], Rosenlicht gave the following example of a wound noncommutative unipotent group G over a non-perfect field of characteristic 3. We are interested in computing its Galois cohomology in degree 1 and show that there are many cases where the cohomology is infinite.

4.10. Example. Let k be a non-perfect field of characteristic $p > 2$. Let a be an element of k such that $1, a, a^2$ are linearly independent over k^p. Let

$$\Gamma = \{(c_1, c_2) \in \mathbf{G}_a^2 | c_1^p + ac_2^p + ac_1 = 0\},$$

$$G_1 = \{(x, y) \in \mathbf{G}_a^2 | y^p - y = ax^p\},$$

$$G_2 = \{(x_1, x_2, x_3) \in \mathbf{G}_a^3 | x_1^p + ax_2^p + a^{-1}x_3^p + x_3 = 0\}.$$

For $\gamma = (c_1, c_2) \in \Gamma$, let

$$\varphi_\gamma(x, y) = \varphi_{(c_1,c_2)}(x, y) = (c_1x - c_2y, c_2x, -c_1y).$$

This yields an homomorphism $\varphi : \Gamma \to \mathrm{Hom}(G_1, G_2)$, $\gamma \mapsto \varphi_\gamma$. On $G := \Gamma \times G_1 \times G_2$, we define the multiplication as follow

$$(\gamma, g_1, g_2)(\gamma', g_1', g_2') = (\gamma + \gamma', g_1 + g_1', g_2 + g_2' + \varphi_\gamma(g_1')).$$

Then G is a wound noncommutative unipotent group. By a direct checking, G_2 is central in G and from the exact sequence $1 \to G_2 \to G \to G/G_2 \to 1$, we have the following exact sequence (of pointed sets)

$$\mathrm{H}^1(k, G_2) \to \mathrm{H}^1(k, G) \to \mathrm{H}^1(k, \Gamma \times G_1) \to 1.$$

When $k = \mathbf{F}_q((t))$, $q = 3^n$, $a = t$, then by Proposition 4.5, $\mathrm{H}^1(k, G_2) = 0$. Then $\mathrm{H}^1(k, G) \simeq \mathrm{H}^1(k, \Gamma \times G_1)$, and $\mathrm{H}^1(k, G)$ has a group structure via this

bijection. In general, by Theorem 4.8, $\mathrm{H}^1(k, G_1)$ is infinite (since $p > 2$), hence so is $\mathrm{H}^1(k, G)$.

4.11. Remark. If $p = 2$ (resp. $p = 3$) then Proposition 4.2 (resp. Proposition 4. 3) shows that there are examples of a global field k and commutative unipotent k-groups G of dimension 1 (resp. 2) where $\mathrm{H}^1(k_v, G)$ is finite , but non-trivial.

Theorem. *Let k be a non-perfect field of charateristic $p > 0$.*
1) *The one-dimensional Galois cohomology $\mathrm{H}^1(k, G)$ of any connected smooth unipotent non-k-split k-group G is non-trivial (resp. infinite) if and only the same is true for connected smooth commutative unipotent k-wound groups of exponent p. In particular, over global function fields k, one-dimensional Galois cohomology of non-split smooth unipotent k-groups of dimension ≤ 1 are always infinite.*
2) *The study of the triviality (resp. finiteness) of $\mathrm{H}^1_{fl}(k, G)$ for unipotent k-group schemes G can be reduced in a canonical way to that for connected smooth commutative k-wound unipotent groups of exponent p.*

Proof. 1) The "Only if" part is trivial.

("If" part.) We assume that the assertion of the theorem holds for one-dimensional smooth unipotent groups. Let G be any smooth unipotent non-split k-group of dimension n. We use induction on n. If $n = 1$, there is nothing to prove, and we assume that $n > 1$ and the assertion holds for all $m < n$. Denote by G_s the k-split part of G. We consider two cases.

a) $G_s \neq 1$. Then G/G_s is unipotent and k-wound as is well-known, and it has dimension strictly less than n. We consider two subcases.

*a*1) If G_s is commutative, we consider the exact sequence of k-groups

$$1 \to G_s \to G \to G/G_s \to 1,$$

and the cohomology sequence derived from this

$$0 \to \mathrm{H}^1(k, G) \xrightarrow{\pi} \mathrm{H}^1(k, G/G_s) \to \mathrm{H}^2(k, G_s) = 0,$$

thus π is surjective. By inductive assumption, $\mathrm{H}^1(k, G/G_s)$ is non-trivial (resp. infinite), so the same is true for $\mathrm{H}^1(k, G)$.

$a2$) Assume that G_s is not commutative. Denote by

$$G_s = G_0 > G_1 > G_2 > \cdots > G_l = \{1\}$$

the derived series of G_s, i.e., $G_{i+1} = [G_i, G_i]$, for all $0 \leq i \leq l-1$, and G_{l-1} is commutative and non-trivial, hence it has positive dimension. One checks that G_{l-1} is a normal subgroup of G and the assertion of the theorem follows from the exact sequence

$$1 \to G_{l-1} \to G \to G/G_{l-1} \to 1$$

by combining with the above arguments.

b) $G_s = 1$, i.e., G is k-wound. If G is commutative and of exponent p, there is nothing to prove. Assume that G is not of this type. Then it is well-known by Tits theory again ([Oe], [Ti]), that there exists a central connected commutative k-subgroup K of G of exponent p with $\dim K > 0$, such that G/K is k-wound. The assertion now follows by using the exact sequence

$$1 \to K \to G \to G/K \to 1$$

and the induction hypothesis.

2) We first use induction on the length of the ascending central series of G. To reduce the length, we consider the center $C(G)$ of G, which is non-trivial, since G is nilpotent. The exact sequence $1 \to C(G) \to G \to G/C(G) \to 1$ will do the job. Therefore we are reduced to the case G is commutative. The exact sequence $1 \to G^\circ \to G \to G/G^\circ \to 1$, combined with Proposition 4.7 reduces the situation further to the case G is connected. Again by using Proposition 4.7, we are reduced to the case G is smooth and connected. Now the rests follows from the last part of the proof of 1). ∎

5 Some local - global principles and applications

We derive from Theorem 3.1 and its proof and from [Oe] the following

5.1. Theorem. (Local - global principle). *Let k be a global field and let G be a smooth group defined over k with finite Shafarevich - Tate group.*
a) If G satisfies the condition $(*)$ of Section 3, then $\mathrm{H}^1(k,G)$ is trivial if and only if $\mathrm{H}^1(k_v,G)$ is trivial for all valuations v of k and for some (hence any) embedding of G into a k-group $H=\mathrm{SL}_n$ such that with natural action of H on H/G, the orbits of $H(k)$ are closed in $(H/G)(k)$ in the $A(S)$-topology of $(H/G)(k)$ for any finite set S of valuations of k.
b) If G is unipotent, then the assertion a) also holds for a k-split unipotent group H.

Proof. In fact we prove a slightly stronger assertion as follows.

$(\bullet)$ *If $\mathrm{H}^1(k,G)$ is trivial, then for any valuation v of k, $\mathrm{H}^1(k_v,G)$ is also trivial. Conversely, if $\mathrm{H}^1(k_v,G)$ is finite for all v and it is trivial for almost all v, and if the above embedding condition holds, then $\mathrm{H}^1(k,G)$ is also trivial.*

Proof of $(\bullet)$. The first part of the statement is trivial in the case a) and follows from the proof given above in Section 3 for the case b). For the second one, recall that for smooth k-group G, the Tate - Shafarevich group

$$Ш(G) := \mathrm{Ker}\,(\mathrm{H}^1(k,G) \to \prod_v \mathrm{H}^1(k_v,G))$$

is finite according to [Oe], Chap. IV, Prop. 2.6. It follows easy from Corollary 3.4 that for any finite set S of valuations of k, the localization map

$$\varphi_S : \mathrm{H}^1(k,G) \to \prod_{v\in S} \mathrm{H}^1(k_v,G)$$

is surjective (in fact a more general result holds true, see [TT]). We take $S := \{\ v \mid \mathrm{H}^1(k_v,G) \neq 0\}$ (which may be empty); then we have an exact sequence of abelian groups

$$1 \to Ш(G) \to \mathrm{H}^1(k,G) \to \prod_{v\in S} \mathrm{H}^1(k_v,G) \to 1.$$

From this and from the assumption it follows that $\mathrm{H}^1(k,G)$ is finite as well, and by our theorem, $\mathrm{H}^1(k,G)$ is trivial as required. ∎

With above notation we have also the following

5.2. Corollary. *a) If T is a smooth k-torus, K a finite radicial (i.e. purely inseparable) extension of k of degree p^n, and $G = R_{K/k}(T_K)$, then the k-group $U := G/T$ has trivial (resp. finite) 1-Galois cohomology if and only if both groups $\mathrm{H}^1(k,T)/p^n$ and ${}_{p^n}\mathrm{H}^2(k,T)$ are trivial (resp. finite).*
b) For any smooth k-torus T and finite set S of non-equivalent valuations of k, the localization map

$$ {}_{p^n}\mathrm{H}^2(k,T) \to \coprod_{v\notin S} {}_{p^n}\mathrm{H}^2(k_v,T) $$

is surjective.
c) If T, G and U are as in a), then for U the obstruction to weak approximation in S is finite, i.e., the quotient $\mathrm{A}(S,U) = \prod_{v\in S} U(k_v)/Cl(U(k))$ is a finite abelian group.

Here for an abelian group A and a natural number n we denote by A/n (resp. ${}_nA$) the cokernel (resp. kernel) of the natural endomorphism $A \stackrel{\times n}{\to} A, x \mapsto nx$.

Proof. *a*) According to [Oe], Appendix 3, U is a smooth unipotent group, and by loc.cit, Chap. VI, Sec. 5.2, we have the following exact sequence

$$ \mathrm{H}^1(k,T) \stackrel{p^n}{\to} \mathrm{H}^1(k,T) \to \mathrm{H}^1(k,U) \to \mathrm{H}^2(k,T) \stackrel{p^n}{\to} \mathrm{H}^2(k,T), $$

thus we have also an exact sequence

$$ 0 \to \mathrm{H}^1(k,T)/p^n \to \mathrm{H}^1(k,U) \to {}_{p^n}\mathrm{H}^2(k,T) \to 0. $$

Hence $\mathrm{H}^1(k,U)$ is trivial (resp. finite) if and only if both groups $\mathrm{H}^1(k,T)/p^n$ and ${}_{p^n}\mathrm{H}^2(k,T)$ are trivial (resp. finite).

b) Follows from the exact sequence above and Corollary 3.4.

c) We prove a more general assertion. Namely

(#) *if U is a k-unipotent group for which there is a separable dominant k-morphism $f : V \to U$, where V is an open set in some affine space $\mathbf{A}^n$*

then the assertion of the corollary holds.

Indeed, by Implicit Function theorem (see [Se2, Part 2]), being separable, f defines open maps $f_v : V(k_v) \to U(k_v)$ for all valuations v of k, according to implicit function theorem. Since $V(k)$ is dense in $\prod_{v\in S} V(k_v)$, it follows that $Cl(f(V(k)))$ is open in $\prod_{v\in S} U(k_v)$ and so is $Cl(U(k))$. Therefore $\mathrm{A}(S,U)$ is discrete in its natural quotient topology. If U is k-wound then $U(k_v)$ is compact by [Oe], Chap. VI, Prop. 2.1. Therefore $\mathrm{A}(S,U)$ is finite as required. In general case, we have the following exact sequence

$$1 \to U_s \to U \to Q \to 1,$$

where U_s is the maximal k-split normal connected subgroup of U, $Q = U/U_s$ (see [Ti], [Oe]). We apply Lemma 3.3 above to the following commutative diagram

$$\begin{array}{ccccccc} U_s(k) & \to & U(k) & \to & Q(k) & \to & 1 \\ \alpha\downarrow & & \downarrow\beta & & \downarrow\gamma' & & \\ U_s(S) & \to & U(S) & \to & Q(S) & \to & 1 \end{array}$$

where $X(S) := \prod_{v\in S} X(k_v)$, with X stands for U, U_s, Q, and $U_s(k)$ is dense in $U_s(S)$ due to weak approximation in the k-split group U_s. We have a homeomorphism

$$\begin{aligned} \mathrm{A}(S,U) &= U(S)/Cl(U(k)) \\ &\simeq Q(S)/Cl(Q(k)) \\ &= \mathrm{A}(S,Q). \end{aligned}$$

Since Q is k-wound ([Ti], [Oe]), then for any valuation v, $Q(k_v)$ is compact ([Oe], loc.cit.), thus $\mathrm{A}(S,Q)$ is also compact. Since $\mathrm{A}(S,U)$ is discrete (see above), it follows that all they are finite as required.

The group $U = G/T$ satisfies our assumptions in (#) by [Oe], Chap. VI, hence c) holds. ∎

5.3. We now consider some applications to local - global principles for universality of polynomials over global fields. We say that a polynomial $F(T) := F(T_1, ..., T_n) \in k[T_1, ..., T_n]$ is *universal* over k if it represents any element from k, i.e., the equation $F(T) = a$ has solution in k^n for any $a \in k$. As an easy consequence of the Hasse - Minkowski theorem (local - global principle) for quadratic forms we have the following (perhaps well-known)

Proposition. *Let $f = f(X_1, ..., X_n)$ be a quadratic form in n variables over a global field of characteristic $p \neq 2$. Then f is universal over k if and only if f is so over all completions k_v of k.*

Proof. Assume that f is universal over k. It is clear that k_v^{*2} is open in k_v. For any $b_v \in k_v^*$ we pick $b \in k^*$ such that b is sufficiently close to b_v in the v-adic topology, and so that $b_v = bc_v^2$, where $c_v \in k_v^*$. Since $f(k^n) = k$ by assumption, we see that there is $a \in k^n$ such that $f(a) = b$, hence $f(c_v a) = bc_v^2 = b_v$, i.e., f is also universal over k_v.

Conversely, assume that f is universal over k_v for all v. Take any $b \in k^*$ and consider the quadratic form $f' := f - bX^2$, where X is a new variable. Since f is universal over k_v for all v, one sees that f represents b over k_v for all v, i.e., the quadratic form f' is isotropic over k_v, for all v. Now Hasse - Minkowski Theorem for quadratic forms over global fields (see e. g. [Sc]) tells us that f' is also isotropic over k. Denote by $(x_1, ..., x_n, x) \in k^{n+1}$ be a non-trivial zero of f'. If $x = 0$, then $(x_1, ..., x_n)$ is a non-trivial zero of f, so f is isotropic over k. Hence f is universal over k and f represents b over k. Otherwise, $x \neq 0$ and we may divide by x^2 to see that again f represents b over k. ∎

5.4. A polynomial $F(T)$ in n variables $T = (T_1, ..., T_n)$ with coefficients in a field k is called *additive*, if $F(X + Y) = F(X) + F(Y)$ for any $X, Y \in k^n$. Clearly, any algebraic group morphism from vector groups to the additive group $\mathbf{G}_a$ is an additive polynomial. It is well-known (see e. g. [Go], [W1, W2]) that additive polynomials play important role in the study of arithmetic of the global function fields. In particular, its universality plays also some role in the model-theoretic approach to the arithmetic of function fields (cf. e. g. [Ku]).

Theorem. *Let F be a separable additive polynomial in n variables with coefficients in a global field k.*
a) F is universal over k if and only if F is universal over k_v for all valuations v of k, and $F(k^n)$ is $A(S)$-closed in k for all finite set S of valuations of k .
b) Assume that n=2. Then F is universal over K if and only if it is so over all k_v.

Proof. *a)* By assumption, F can be regarded as a separable morphism of algebraic groups $F : \mathbf{G}_a^n \to \mathbf{G}_a$. The kernel of F is then a commutative smooth unipotent k-subgroup G_F of $\mathbf{G}_a^n$, and we have the following exact sequence of k-groups

$$1 \to G_F \to \mathbf{G}_a^n \xrightarrow{F} \mathbf{G}_a \to 1.$$

It is well-known that F is a p-polynomial, where p is the characteristic of the field k. Thus if $p = 0$, there is nothing to prove. Let $p > 0$. The exact sequence of Galois cohomology related to the exact sequence above gives us the first Galois cohomology of G_F as follows : For any extension field K/k we have

$$\mathrm{H}^1(K, G_F) \simeq K/F(K^n).$$

Thus our additive polynomial F is universal over a field K if and only if $\mathrm{H}^1(K, G_F) = 1$. Therefore, from Theorem 5.1 it follows that over a global field k, an additive separable polynomial is universal over k if and only if it is so over all completions k_v of k and the condition regarding the closedness holds.
b) With notation as in the proof of *a)*, G_F is a connected and smooth unipotent k-group of dimension 1. If $\mathrm{H}^1(k, G_F) = 1$, then from the surjectivity of the localization map we know that $\mathrm{H}^1(k_v, G) = 1$ for all v.

Conversely, assume that $\mathrm{H}^1(k_v, G_F) = 1$ for all v. Assume first that $p \neq 2$. Then it follows from the exact sequence

$$1 \to Ш(G_F) \to \mathrm{H}^1(k, G_F) \to \prod_v \mathrm{H}^1(k_v, G_F) \to 1$$

and the finiteness of $Ш(G_F)$ ([Oe], Ch. IV) that $\mathrm{H}^1(k, G_F)$ is also finite. Now from Proposition 4.6 it follows $\mathrm{H}^1(k, G_F)$ is either trivial or infinite, hence $\mathrm{H}^1(k, G_F) = 1$ as required. Therefore F is universal over k if and only if it is so over all k_v.

Let $p = 2$. If G_F were not isomorphic to $\mathbf{G}_a$ then from Propositions 4.2 and 4.6 it would follow that $\mathrm{H}^1(k, G_F)$ is infinite, so $G_F \simeq \mathbf{G}_a$, and the proposition follows. ∎

5.5. Remarks. 1) The "only if" part of Theorem 5.1 in fact, holds true for any field as it follows from a more general result in [TT].

2) One cannot replace the statement regarding the universality (i.e., the representation of *all* elements of k by F) of the additive polynomial F considered by the statement regarding the representation of *an* element of k by F. Namely, using [Oe], Chap. V, one can construct a p-polynomial F and an element $a \in k$ such that the equation $F(T_1, ..., T_n) = a$ has solutions in k_v^n locally everywhere, but has no solutions in k^n, i.e., the local - global principle fails in this case.

The structure of p-polynomials reflects deep arithmetic properties of the base field. As an easy consequence of the above we have

5.6. Corollary. *Let k be a non-perfect field of characteristic $p > 0$. Then, for any n, k has cyclic extensions of degree p^n.*

Proof. By Proposition 4.7, for any k-form G of $\mathbf{F}_p$, the Galois cohomology $\mathrm{H}^1(k, G)$ is infinite. In particular, there exists $\alpha \in k \setminus \wp(k)$, where $\wp(x) = x^p - x$ is the Artin - Schreier polynomial. By a well-known theorem of Witt [Wi, Satz 13], for any n there exist cyclic extensions of k of degree p^n. ∎

5.7. Remark. P. Russell showed in [Ru], p. 538, that

(∗) *if a field k of characteristic $p > 0$ does not have normal extensions of degree p, then for any p-polynomial $f(T) = a_0T + a_1T^p + \cdots + a_mT^{p^m} \in k[T]$, with $a_0 \neq 0$, we have $f(k) = k$, and $\mathrm{H}^1(k, G) = 0$ for all G which are k-forms of $\mathbf{G}_a$.*

In other words, for the following statements

a) k has no normal extensions of degree p;

b) every separable p-polynomial $f(T) = a_0T + a_1T^p + \cdots + a_mT^{p^m}$ *(*$a_0 \neq 0$*) is universal, i.e.,* $f(k) = k$*;*

c) Every k-form G of $\mathbf{G}_a$ *has trivial 1-Galois cohomology,*

we have the following implications

$$a) \Rightarrow b) \Rightarrow c).$$

Equivalently, if the field k is such that there is a k-form G of $\mathbf{G}_a$ with non-trivial 1-cohomology, then k has a normal extension of degree p. (This can be derived immediately from Corollary 5.6, since such a field k must be non-perfect, according to Rosenlicht' Theorem, hence by Corollary 5.6 it has cyclic extensions of degree p^n for any n.) There (in [Ru], p. 538) it was also mentioned that *"the author does not know whether the converse of this statement is true if k is not perfect."*

In other words, one may wonder if the following implications are true if k is not perfect :

$$c) \Rightarrow b) \Rightarrow a).$$

Our result (Proposition 4.6) gives a clarification to this question. Namely, with the assumption on the non-perfectness of k, it is automatically true that k has normal extensions of degree p, and that there are k-forms G of $\mathbf{G}_a$ with non-trivial one-dimensional Galois cohomology. Therefore the above implications also hold true.

Acknowledgements. We would like to thank T. Kambayashi, J. Oesterlé and P. Russell for their attention and support via email correspondences. The first author would like to thank the Abdus Salam I. C. T. P. and I. H. E. S. for the support and excellent working condition while preparing this version of the paper.

References

[Bo] A. Borel, *Linear algebraic groups* (second enlarged version), GTM 126, Springer - Verlag, 1991.

[BH] A. Borel and G. Harder, Existence of discrete cocompact subgroups of reductive groups over local fields, J. reine und angew. Math., Bd. 298 (1978), 53 - 64.

[Bou] N. Bourbaki, *Algèbre commutative*, Hermann - Paris, 1972.

[Ca] P. Cartier, Inseparable Galois cohomology, in : "Algebraic Groups and Discontinuous Subgroups", A. M. S. Proceedings in Pure Math. v. 9 (1966), 183 - 186.

[DG] M. Demazure et P. Gabriel, *Groupes algébriques*, Tome I, Paris, Masson, 1970.

[Go] D. Goss, *Basic structure of function field arithmetic*, Springer - Verlag, 1996.

[Gr] A. Grothendieck, *Fondaments de la Géométrie Algébrique*, Institut Henri Poincaré, Paris, 1958.

[Gr-D] A. Grothendieck (avec la collaboration de J. Dieudonné), Éléments de la Géométrie Algébrique, *Pub. Math. I. H. E. S.*, Ch. IV, No. 20, 24, 28, 32, 1964 - 1967.

[Ha] G. Harder, Über die Galoiskohomologie der halbeinfacher Matrizengruppen, III, J. reine und angew. Math., Bd. 274/275 (1975), 125 - 138.

[KMT] T. Kambayashi, M. Miyanishi and M. Takeuchi, *Unipotent algebraic groups*, Lecture Notes in Math. v. 414, Springer - Verlag, 1974.

[Kn] M. Kneser, *Lectures on Galois cohomology of classical groups*, Tata Inst. Fund. Res., Bombay, 1969.

[Ku] F. -V. Kühlmann, Valuation theoretic and Model theoretic aspects of local uniformization, in : *"Resolution of Singularities"*, Progress in Math., v. 181 (2000), 381 - 456.

[La] S. Lang, Algebraic groups over finite fields, *Amer. J. Math.*, v. 78 (1958), 553 - 563.

[Mi1] J. S. Milne, *Étale cohomology*, Princeton University Press, 1980.

[Mi2] J. S. Milne, *Arithmetic Duality Theorems* (second ed.), version of March 2004.

[PR] V. Platonov and A. Rapinchuk, *Algebraic groups and Number theory,* Academic Press, 1994.

[Oe] J. Oesterlé, Nombre de Tamagawa et groupes unipotents en carateristique p, *Invent. Math.* v. 78 (1984), 13 - 88.

[Ro1] M. Rosenlicht, Some rationality questions on algebraic groups, *Annali di Mat. Pura ed Appl.*, v. 43 (1957), 25 - 50.

[Ro2] M. Rosenlicht, Questions of rationality for solvable algebraic groups over non-perfect fields, *Annali di Mat. Pura ed App.* v. 61 (1963), 97 - 120.

[Ru] P. Russell, Forms of the affine line and its additive groups, *Pacific J. Math*, v. 32 (1970), 527 - 539.

[Sc] W. Scharlau, *Quadratic and Hermitian Forms,* Springer - Verlag, 1985.

[Se1] J. -P. Serre, *Cohomologie Galoisienne* (cinquième éd.), Lecture Notes in Math. v. 5, Springer - Verlag, 1994.

[Se2] J. -P. Serre, *Lie algebras and Lie groups*, Harvard Univ. Lecture Notes, Benjamin, 1964.

[Sh] S. Shatz, Cohomology of Artinian group schemes over local fields, *Annals of Mathematics* v. 79 (1964), 411 - 449.

[SGA 3] M. Demazure et al., *Schémas en groupes*, Lecture Notes in Mathematics, vols. 151, 152, 153, Springer - Verlag, 1970.

[SGA 4] M. Artin et al., *Théorie des topos et cohomologie étale des schemas,* Lec. Notes in Math. 269, 270, 305, Springer - Verlag, 1970.

[T] Nguyen Q. Thang, On Corestriction Principle for non-abelian Galois cohomology over local and global fields. II. $Char.p > 0$. Preprint, 2004.

[TT] Nguyen Q. Thang and Nguyen D. Tan, On the surjectivity of the localisation maps for Galois cohomology of algebraic groups over fields, Commun. Algebra, v. 32 (2004), 3169 - 3177.

[Ti] J. Tits, *Lectures on Algebraic Groups*, Yale Univ., 1967.

[We] A. Weil, *Basic Number Theory*, Grundlehren der Wiss. Math., v. 144, Springer - Verlag, 1995.

[W1] G. Whaples, Additive polynomials, *Duke Math. J.*, v. 21 (1954), 55 - 65.

[W2] G. Whaples, Galois cohomology of additive polynomial and n-th power mappings of fields, *Duke Math. J.* , v. 24 (1957), 143 - 150.

[W3] G. Whaples, Algebraic extensions of arbitrary fields, *Duke Math. J.*, v. 24 (1957), 201 - 204.

[Wi] E. Witt, Zyklische Körper und Algebren der Characteristik p und von grad p^n. Struktur diskret bewerteter Körper mit vollkommenem Restklassenkörper der Charakteristik p, *J. Reine. Angew. Math.* 176 (1937), 126 - 140.