REDUCTION OF STRUCTURE FOR TORSORS OVER SEMILOCAL RINGS

V. CHERNOUSOV, P. GILLE, AND Z. REICHSTEIN

Abstract. Let G be a reductive affine group scheme defined over a semilocal ring k. Assume that either G is semisimple or k is normal and noetherian. We show that G has a finite k-subgroup S such that the natural map $H^1(R, S) \to H^1(R, G)$ is surjective for every semilocal ring R containing k. In other words, G-torsors over $\mathrm{Spec}(R)$ admit reduction of structure to S. We also show that the natural map $H^1(X, S) \to H^1(X, G)$ is surjective in several other contexts, under suitable assumptions on the base ring k, the scheme X/k and the group scheme G/k. These results have already been used to study loop algebras and essential dimension of connected algebraic groups in prime characteristic. Additional applications are presented at the end of this paper.

Contents

1. Introduction

Let G be a linear algebraic group defined over a field k. In [CGR] we showed that, under mild assumptions on G and k, G has a finite k-subgroup

1991 *Mathematics Subject Classification.* 11E72, 14L15, 20G10.

Key words and phrases. Linear algebraic group, group scheme, torsor, non-abelian cohomology.

V. Chernousov was partially supported by the Canada Research Chairs Program and an NSERC research grant.

Z. Reichstein was partially supported by NSERC Discovery and Accelerator Supplement grants.

S such that every G-torsor over a field K/k admits reduction of structure to S, i.e., the natural map of Galois cohomology sets $H^1(K,S) \to H^1(K,G)$ is surjective. In several subsequent applications, a more general version of this result was needed, with the field k replaced by a base ring, the group G by a reductive group scheme over k and the field K/k by a k-scheme X. The goal of this paper is to extend the main result of [CGR] to this more general setting.

All schemes in this paper will be assumed to be locally noetherian. Of particular interest to us will be k-schemes X satisfying the following condition:

$$\text{Pic}(X') = 0 \text{ for every generalized Galois cover } X'/X. \tag{1.1}$$

Here by a generalized Galois cover $X' \to X$ we mean a Γ-torsor, for some twisted finite constant group scheme Γ defined over X. In other words, $\Gamma = {}_aC$, where C is a finite constant group scheme over X and $[a] \in H^1(X, \text{Aut}(C))$. (The term "Galois cover" is usually reserved for the case where Γ is itself a finite constant group scheme.) The class of schemes satisfying condition (1.1) includes, in particular, affine schemes of the form $X = \text{Spec}(R)$, where R is a semilocal ring containing k. If K is a k-field of characteristic 0, we can also take R to be a polynomial ring $K[x_1, \dots, x_n]$ (see §8) or a Laurent polynomial ring $K[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ (see Remark 8.3).

We are now ready to state the main results of this paper. Recall that an X-group T of multiplicative type is called *isotrivial* if $T \times_X X'$ is split for some finite étale surjective map $X' \to X$. For the definition and basic properties of groups of multiplicative type, we refer the reader to [SGA3, X].

1.2. **Theorem.** *Let k be a commutative base ring and G be a smooth affine group scheme over k whose connected component G^0 is reductive. Assume further that one of the following holds:*

(a) k is an algebraically closed field, or

(b) $k = \mathbb{Z}$, G^0 is a split Chevalley group, and the order of the Weyl group of the geometric fiber $G_{\overline{s}}$ is independent of $s \in \text{Spec}(\mathbb{Z})$, or

(c) k is a semilocal ring, G is connected, and the radical torus rad(G) *is isotrivial.*

Then there exist a maximal torus $T \subset G^0$ defined over k and a finite k-subgroup $S \subset N_G(T)$, such that

1. *S is an extension of a twisted constant group scheme by a finite k-group of multiplicative type,*
2. *the natural map $H^1(X,S) \longrightarrow H^1(X, N_G(T))$ is surjective for any scheme X/k satisfying condition* (1.1)*.*

Of course, if G is connected then (a) is a special case of (c). Note also that in case (b) we can take G to be the automorphism group $\text{Aut}(G_0)$ of some semisimple Chevalley group scheme G_0. In this case the cohomology set

$H^1(X, G)$ classifies the semisimple group schemes over X, which are étale locally isomorphic to $G_0 \times_{\mathbb{Z}} X$.

Combining Theorem 1.2(c) with Grothendieck's existence theorem for maximal tori (reproduced as Theorem 5.2 below), we obtain the following stronger result in case (c); cf. §7.

1.3. **Theorem.** *Let k, G and S be as in Theorem 1.2(c). Then the map $H^1(R, S) \to H^1(R, G)$ is surjective for any semilocal ring R/k.*

Note that the assumption on the radical of G is superfluous if G is a semisimple group scheme or if k is normal and noetherian, because all tori defined over such rings are isotrivial; see [SGA3, X.5.16].

The symbol $H^1(X, G)$ in the statements of Theorems 1.2 and 1.3 denotes the flat cohomology set, which classifies G-torsors over X; see §2. If G is smooth then every G-torsor over X is also smooth and is trivialized by an étale covering [M, III.4]. So in this case the natural map $H^1_{ét}(X, G) \to H^1(X, G)$ is bijective, and we may replace $H^1(X, G)$ by $H^1_{ét}(X, G)$.

In particular, suppose that k is an algebraically closed field and G/k and S/k are as in Theorem 1.2(a). If K is a perfect field containing k and K_s is the separable closure of K then

$$H^1(K, G) = H^1(\mathrm{Gal}(K_s/K), G(K_s))$$

and

$$H^1(K, S) = H^1(\mathrm{Gal}(K_s/K), S(K_s))\,.$$

In other words, in this situation the flat cohomology sets appearing in the statement of Theorem 1.2(a) can be replaced by Galois cohomology. Moreover, since S is finite, $S(k) = S(K_s)$ (with $\mathrm{Gal}(K_s/K)$ acting trivially on both sides) and hence,

$$H^1(\mathrm{Gal}(K_s/K), S(k)) = H^1(\mathrm{Gal}(K_s/K), S(K_s))\,.$$

Thus in this setting Theorem 1.2(a) implies the following characteristic-free result about Galois cohomology. The assertion about $|S| := \dim_k k[S]$ is immediate from the construction of S in §4.

1.4. **Corollary.** *Let G be a smooth linear algebraic group defined over an algebraically closed field k, whose connected component G^0 is reductive. Then there exists a finite k-subgroup S of G, such that every prime factor of $|S|$ divides the order of the Weyl group $W(G)$, and the map*

$$H^1(\mathrm{Gal}(K_s/K), S(k)) \to H^1(\mathrm{Gal}(K_s/K), G(K_s))$$

is surjective for any perfect field K/k. □

Corollary 1.4 generalizes [CGR, Theorem 1.1(a)], which yields the same conclusion if $\mathrm{char}(k) = 0$. This corollary has been used to study essential dimension of connected algebraic groups in positive characteristic in [GR]. An application of Theorem 1.2 to the study of loop algebras can be found in [GP]; cf. Remark 8.3. We will give additional applications in §§ 7 and 8.

A further application of Theorem 1.2 will appear in the forthcoming paper [CGP].

Acknowledgments. We are grateful to M. Florence for pointing out a mistake in the proof of [CGR, Theorem 1.1(a)]. This mistake is corrected in the course of the proof of Lemma 3.2. For details, see Remark 4.1.

We would also like to thank the referee for helpful remarks.

2. Preliminaries

We begin by recalling some known facts about flat affine group schemes G of finite type over an arbitrary base scheme X.

A pseudo G-torsor (*formellement principal homogène*, in [SGA3]) E over X is an X-scheme equipped with a right action of G such that the mapping $E \times_X G \to E \times_X E$ given by $(x, g) \mapsto (x, x.g)$ is an isomorphism; see [SGA3, IV.5.1]. A pseudo G-torsor E is *a G-torsor* (*fibré principal homogène*) if it is locally trivial in the fppf topology, i.e., if there exists a faithfully flat morphism $X' \to X$, locally of finite type, such that $E \times_X X' \cong G \times_X X'$. Here, as usual, the acronym fppf stands for "fidèlement plate de présentation finie" or "faithfully flat and finitely presented".

For such a covering $X' \to X$, we define

$$Z^1(X'/X, G) := \left\{ g \in G(X' \times_X X') \mid p_{1,2}^*(g) p_{2,3}^*(g) = p_{1,3}^*(g) \right\}$$

and

$$H^1(X'/X, G) := Z^1(X'/X, G)/G(X'),$$

where $G(X')$ acts on $Z^1(X'/X, G)$ by $g \cdot z = p_1^*(g)\, z\, p_2^*(g)^{-1}$; see [K, Chapter III]. Here $p_{i,j} \colon X' \times_X X' \times_X X' \to X' \times_X X'$ is the projection

$$(x_1', x_2', x_3') \to (x_i', x_j')\,,$$

and $p_{1,2}^*(g)$, $p_{2,3}^*(g)$, $p_{1,3}^*(g)$ are viewed as elements of $G(X' \times_X X' \times_X X')$. The pointed set $H^1(X'/X, G)$ classifies G-torsors over X which are trivialized by the base change X'/X, i.e., G-torsors E satisfying

$$E \times_X X' \xrightarrow{\sim} G \times_X X'\,;$$

see [M, III.4, page 120]. We now define

$$H^1(X, G) := \varinjlim_{X'} H^1(X'/X, G)\,,$$

where the limit is taken over all coverings X'/X in the $fppf$ topology. The pointed set $H^1(X, G)$ classifies G-torsors over X.

If P is a G-torsor over X, we denote by ${}^P G$ the associated twisted X-group scheme; it is the twisted inner form of G and can be defined as the scheme of G-automorphisms of P. We then have a canonical bijection (the "torsion" map)

$$H^1(X, G) \xrightarrow{\simeq} H^1(X, {}^P G)$$

mapping a G-torsor Q to $\underline{\mathrm{Isom}}_G(P,Q)$; see [Gir, III.2.6]. More precisely, the fppf sheaf of sets $\underline{\mathrm{Isom}}_G(P,Q)$ of G-isomorphisms of P into Q is a G-torsor which is representable by an affine scheme over S by faithfully flat descent [M, th. IV.4.3]. In particular, the torsion map takes P to the trivial ${}^PG$-torsor.

We say that G is *connected* if the fiber G_x is connected for any point $x \in X$. Here we view $G_x = G \times_X \mathrm{Spec}(\kappa(x))$ as an algebraic group over the residue field $\kappa(x)$ of x. If G/X is smooth, then G contains a unique maximal open connected normal subgroup defined over X; [SGA3, VI_B, Thm. 3.10]. As usual, we will denote this subgroup by G^0/X and refer to it as *the connected component* of G. Note that G^0 is smooth over X and it is a closed subgroup of G; in particular, it is affine over X.

We say that G/X is *reductive* if it is smooth and all of its geometric fibers $G_{\overline{x}}$ are (connected) reductive groups [SGA3, XIX.2.7]. A subgroup T/X of G/X is a *maximal torus* if it is an X-torus and all of its geometric fibers are maximal tori [SGA3, XII.1.3]. The *radical torus* $\mathrm{rad}(G)$ of G is the unique maximal torus of the center of G [SGA3, XXII.4.3.6].

Following [SGA3, XXII.5.2.3, XXVI.1] we will say that a subgroup B/X of a reductive group scheme G/X is a *Borel subgroup* if it is smooth [SGA4, §17.3] and all of its geometric fibers are Borel subgroups.

We refer to [SGA3, XXII.1] for the definitions of split group schemes and to [SGA3, XXIV.3] for the definition of the Dynkin scheme of G and quasi-split reductive group schemes.

Let G be a split adjoint semisimple group over X, T a maximal split torus in G defined over X, B a Borel subgroup containing T and D/X the corresponding Dynkin scheme of G. Following [SGA3, XXIV.3.5], we will denote the group scheme representing the functor of automorphisms of D (as a Dynkin scheme) by $\mathrm{Aut}_{Dyn}(D)$. By [SGA3, XXIV, Théorème 1.3 and 3.6]

$$\mathrm{Aut}(G) = G \rtimes \mathrm{Aut}_{Dyn}(D)\,.$$

Moreover, there exists a canonical splitting

$$h\colon\ \mathrm{Aut}_{Dyn}(D) \to \mathrm{Aut}(G)$$

such that the image of h preserves T and B. Every quasi-split adjoint group scheme G' of the same type as G is X-isomorphic to the twist ${}_{h_*(a)}G$ of G for some cocycle

$$a \in Z^1_{\acute{e}t}(X, \mathrm{Aut}_{Dyn}(D))\,.$$

3. A first step towards the proof of Theorem 1.2

The purpose of this section is to prove the following proposition, which will play a key role in the proof of Theorem 1.2.

3.1. **Proposition.** *Let k be a commutative base ring and*

$$1 \to T \to N \xrightarrow{p} W \to 1$$

be an exact sequence of smooth group schemes defined over k, where T is an isotrivial torus, split by a Galois extension k'/k of degree d, and W is a twisted finite constant group of order n. Suppose N has a finite k-subgroup S' such that $p(S') = W$. Then there exists a finite k-subgroup $S \subset N$ containing S' such that the natural map $H^1(X, S) \to H^1(X, N)$ is surjective for any k-scheme X satisfying condition (1.1).

Moreover, we can take S to be the subgroup of N generated by S' and $\phi_m^{-1}(S' \cap T)$, where $m = nd$ and $\phi_m \colon T \to T$ is the map taking $t \in T$ to t^m.

Proof. Denote by $q \colon S \to W$ and $q' \colon S' \to W$ the restrictions of the projection $p \colon N \to W$ to S and S', and by $\mu = S \cap T$ and $\mu' = S' \cap T$ the kernels of these maps, respectively. Let X be a k-scheme satisfying condition (1.1) on Picard groups. We will prove the surjectivity of $H^1(X, S) \to H^1(X, N)$ fiberwise, with respect to the mapping $p_* : H^1(X, N) \to H^1(X, W)$ induced by p. Fix $[b] \in H^1(X, N)$; our goal is to show that $[b]$ lifts to $H^1(X, S)$.

3.2. **Lemma.** *Let $[a] = p_*([b]) \in H^1(X, W)$. Then*

$$[a] \in \operatorname{Im}(H^1(X, S) \xrightarrow{q_*} H^1(X, W)).$$

Proof of Lemma 3.2. The obstruction to lifting $[a]$ to $H^1(X, S)$ is the class

$$\Delta([a]) \in H^2(X, {}_a\mu),$$

where ${}_a\mu$ denotes the group μ twisted by the torsor a [Gir, IV.4.2.8]. We now use the commutative diagram

$$(3.3) \qquad \begin{array}{ccccccccc} 1 & \longrightarrow & \mu' & \longrightarrow & S' & \xrightarrow{q'} & W & \longrightarrow & 1 \\ & & \cap & & \cap & & || & & \\ 1 & \longrightarrow & \mu & \longrightarrow & S & \xrightarrow{q} & W & \longrightarrow & 1 \\ & & \cap & & \cap & & || & & \\ 1 & \longrightarrow & T & \longrightarrow & N & \xrightarrow{p} & W & \longrightarrow & 1 \end{array}$$

with exact rows and the functoriality of the obstruction $\Delta([a])$. If $\Delta'([a]) \in H^2(X, {}_a\mu')$ is the obstruction to lifting $[a]$ to $H^1(X, S')$, via $q'_* : H^1(X, S') \to H^1(X, W)$, then $\Delta([a])$ is the image of $\Delta'([a])$ under the natural map $H^2(X, {}_a\mu') \to H^2(X, {}_a\mu)$.

The commutative diagram

$$(3.4) \qquad \begin{array}{ccccccccc} 1 & \longrightarrow & {}_a\mu' & \longrightarrow & {}_aT & \xrightarrow{t \mapsto (t \bmod \mu')} & {}_a(T/\mu') & \longrightarrow & 1 \\ & & \cap & & || & & \downarrow & & \\ 1 & \longrightarrow & {}_a\mu & \longrightarrow & {}_aT & \xrightarrow{t \mapsto (t^m \bmod \mu')} & {}_a(T/\mu') & \longrightarrow & 1 \end{array}$$

with exact rows gives rise to the commutative exact diagram

$$\begin{array}{ccccc} H^1(X,\,{}_a(T/\mu')) & \longrightarrow & H^2(X,\,{}_a\mu') & \longrightarrow & H^2(X,\,{}_aT) \\ {\scriptstyle\times m}\downarrow & & \downarrow & & || \\ H^1(X,\,{}_a(T/\mu')) & \longrightarrow & H^2(X,\,{}_a\mu) & \longrightarrow & H^2(X,\,{}_aT) \end{array}$$

which we will now analyze. Recall that the middle vertical map sends $\Delta'([a]) \in H^2(X,\,{}_a\mu')$ to $\Delta([a]) \in H^2(X,\,{}_a\mu)$. Since we are given that $[a]$ lifts to $[b] \in H^1(X, N)$, we have

$$\Delta'([a]) \in \ker\Big(H^2(X, {}_a\mu') \to H^2(X, {}_aT)\Big)$$

and thus

$$\Delta'([a]) \in \mathrm{Im}\,\Big(H^1(X, {}_a(T/\mu')) \to H^2(X, {}_a\mu')\Big).$$

In order to prove the lemma (i.e., to prove that $\Delta([a]) = 0$), it now suffices to show that the vertical map

$$\begin{array}{c} H^1(X,\,{}_a(T/\mu')) \\ {\scriptstyle\times m}\downarrow \\ H^1(X,\,{}_a(T/\mu')) \end{array} \tag{3.5}$$

in the above diagram is trivial.

If $p : X' \to X$ is a cover (i.e., a finite étale map) of degree m and H is a commutative affine X-group scheme, we will denote the trace morphism by $N_{X'/X} : \mathrm{R}_{X'/X}(H) \to H$; cf. [CTS, 0.4]. If p has degree m, the composition

$$H \longrightarrow \mathrm{R}_{X'/X}(H) \xrightarrow{N_{X'/X}} H$$

of $N_{X'/X}$ with the natural map $H \to \mathrm{R}_{X'/X}(H)$ is multiplication by m.

Now let $Y \to X$ be the W-torsor associated to a and apply the above facts to the generalized Galois covering $X' = Y \times_k k' \to X$ of degree $m = nd$, with $H = {}_a(T/\mu')$. Note that this covering trivializes a and splits T. The map (3.5) can be decomposed as

$$H^1(X, {}_aT) \longrightarrow H^1(X, \mathrm{R}_{X'/X}({}_a(T/\mu'))) \longrightarrow H^1(X, {}_a(T/\mu')).$$

Shapiro's lemma and condition (1.1) imply that

$$H^1(X, \mathrm{R}_{X'/X}({}_a(T/\mu'))) = H^1(X', {}_a(T/\mu')) = \mathrm{Pic}\,(X')^{\mathrm{rank}(T)} = 0\,.$$

Hence the map (3.5) is trivial, as claimed. The proof of Lemma 3.2 is now complete. □

We are now ready to finish the proof of Proposition 3.1. Let $[c] \in H^1(X, S)$ be such that $q_*([c]) = [a]$. The bottom two rows of (3.3) give rise to the diagram

$$\begin{array}{ccc} H^1(X, {}_c\mu) & \longrightarrow & q_*^{-1}(a) \subset H^1(X,S) \\ f\downarrow & & \downarrow \\ H^1(X, {}_cT) & \longrightarrow & p_*^{-1}(a) \subset H^1(X,N) \end{array}$$

where the horizontal arrows are the "torsion" maps (see §2). Recall that our goal is to show that $[b] \in p_*^{-1}([a]) \subset H^1(X,N)$ lies in the image of $H^1(X,S)$. If $X = \operatorname{Spec}(K)$ for some field K/k then a twisting argument [Se, I.5.5] shows that the map

$$H^1(K, {}_cT) \to p_*^{-1}([a])$$

is surjective. The same twisting argument goes through for any k-scheme X [Gir, III.3.2.4]; in this case we can also conclude that the map

$$H^1(X, {}_cT) \to p_*^{-1}([a])$$

is surjective. Thus it suffices to prove that the vertical map f in the above diagram is surjective as well. The exact sequence

(3.6) $$1 \longrightarrow {}_c\mu \longrightarrow {}_cT \xrightarrow{t \to (t^m \bmod \mu')} {}_cT/\mu' \longrightarrow 1$$

gives rise to the exact sequence

$$H^1(X, {}_c\mu) \xrightarrow{f} H^1(X, {}_cT) \longrightarrow H^1(X, {}_c(T/\mu')).$$

It thus remains to show that the map

(3.7) $$H^1(X, {}_cT) \to H^1(X, {}_c(T/\mu'))$$

in this sequence is trivial. Indeed, since the group homomorphism

$${}_cT \to {}_c(T/\mu')$$

in (3.6) factors through

$$\times m \colon {}_c(T/\mu') \xrightarrow{\times m} {}_c(T/\mu'),$$

the map (3.7) factors through

$$\times m : H^1(X, {}_c(T/\mu')) \longrightarrow H^1(X, {}_c(T/\mu'))$$

which we showed to be trivial at the end of the proof of Lemma 3.2. We conclude that the map (3.7) is trivial, as claimed. This completes the proof of Proposition 3.1. □

3.8. **Remark.** Let k be a ring, T is a maximal k-torus in an affine algebraic k-group G and $N = N_G(T)$. This is a natural setting, where Proposition 3.1 can be applied. However, it is not a priori clear for which G one can construct a finite group S' as in Proposition 3.1. In fact, it is not even clear in general which affine k-groups G contain a maximal k-torus T. If we can find a maximal k-torus $T \subset G$ and a finite k-subgroup $S' \subset N = N_G(T)$ with desired properties, we would also like to know under what circumstances one can conclude that the map $H^1(X,S) \to H^1(X,G)$ is surjective. In the sequel we will give partial answers to these questions, under additional assumptions on k.

4. Proof of Theorem 1.2(a) and (b)

(a) Let T be a maximal k-torus of G and $N = N_G(T)$. Since

$$N^0 \subset \big(N_{G^0}(T)\big)^0 = T \subset N\,,$$

we have $N^0 = T$. Hence, N is smooth and W is a finite constant group. Let $p\colon N \to W = N/T$ be the natural projection. By Proposition 3.1 it suffices to construct a finite k-subgroup $S' \subset N$ such that $p(S') = W$. In fact, we will construct S' so that μ' be the n-torsion subgroup of T, where $n = |W|$.

Consider the exact sequences

$$1 \to T \to N \overset{p}{\to} W \to 1 \qquad \text{and} \qquad 1 \to \mu' \to T \overset{\times n}{\to} T \to 1\,.$$

According to [DG, II.2, Proposition 2.3] (cf. also [SGA3, XVII, App. I.3.1, page 622]), extensions of W by T are classified by the Hochschild cohomology group $H^2_0(W,T)$. Since W is a constant group scheme, $H^2_0(W,T)$ is isomorphic to the usual cohomology group $H^2(W,T(k))$; see [DG, III.6.4, Proposition 4.2]. Thus the first sequence yields a class in $H^2(W,T(k))$. Since $n \cdot H^2(W,T(k)) = 0$, the second sequence tells us that this class comes from $H^2(W,\mu'(k))$. In other words, there is an extension $S' \subset N$ of W by μ' such that N is the push-out of S' by the morphism $\mu' \hookrightarrow T$. This completes the construction of S'.

(b) Let T be a maximal split torus of G defined over $\mathbb{Z}$. Since the order of the Weyl group of the geometric fiber $G_{\bar{s}}$ is independent of $s \in \operatorname{Spec}(\mathbb{Z})$, by [SGA3, XII.2.1.b], W is represented by a finite étale group scheme over $\mathbb{Z}$. This finite étale group scheme is necessary constant, because $\operatorname{Spec}(\mathbb{Z})$ has trivial fundamental group.

It remains to construct a finite subgroup $S' \subset N$ which surjects onto W; the desired conclusion will then follow from Proposition 3.1.

Our construction of S' will be based on scheme-theoretic adherence, which associates to a closed $\mathbb{Q}$–subscheme $V \subset G_{\mathbb{Q}}$ its Zariski closure $\widetilde{V}$ in $G_{\mathbb{Z}}$. Scheme-theoretic adherence induces a one-to-one correspondence between $\mathbb{Q}$–subchemes of $G_{\mathbb{Q}}$ and flat closed $\mathbb{Z}$–subchemes of $G_{\mathbb{Z}}$ [BT, I.2.6]. In particular, it maps $\mathbb{Q}$–subgroups of $G_{\mathbb{Q}}$ into flat $\mathbb{Z}$–group subschemes of G [BT, I.2.7] (see also [GM, §3]).

Let $T = \mathbb{G}_m^r$, where r is the rank of G. As pointed out by Tits [T], the fact that $H^1(\mathbb{Z},T) = \operatorname{Pic}(\mathbb{Z})^r = 0$ implies that the sequence

$$0 \to T(\mathbb{Z}) \to N(\mathbb{Z}) \to W \to 1.$$

is exact. Since $T(\mathbb{Z}) = \{\pm 1\}^r$, $N(\mathbb{Z})$ is a finite group. View $N(\mathbb{Z})$ as a finite constant $\mathbb{Q}$–subgroup of $G_{\mathbb{Q}}$ and let S' be its scheme-theoretic adherence in $N/\mathbb{Z}$. It comes equipped with a group scheme homomorphism $S' \to W$. Since the $\mathbb{Z}$–group scheme μ_2 is the scheme-theoretic adherence of $\{\pm 1\}$ in

$\mathbb{G}_{m,\mathbb{Z}}$, and μ_2^r is the scheme-theoretic adherence of $T(\mathbb{Z})$ in $T/\mathbb{Z}$ (or equivalently in $N/\mathbb{Z}$), it follows that S' contains μ_2^r as a closed $\mathbb{Z}$-subgroup. The quotient $W' = S'/\mu_2^r$ is representable by an affine $\mathbb{Z}$–group scheme [SGA3, VIII.5.7] which is flat over $\mathbb{Z}$ [SGA3, VI_B.9.2.xi]. Obviously the homomorphism $S' \to W$ is trivial on μ_2^r. We thus get a morphism of $\mathbb{Z}$–group schemes $W' \to W$ such that $W'_{\mathbb{Q}} \xrightarrow{\sim} W_{\mathbb{Q}}$. Since W and W' are flat over $\mathbb{Z}$, we conclude that $W \cong W'$. Thus S' is an extension of W by μ_2^r and thus enjoys the required properties; cf. [SGA3, Expose VIB, Proposition 9.2]. □

4.1. **Remark.** In the case where $X = \mathrm{Spec}(K)$ for some field K/k, Theorem 1.2(a) reduces to [CGR, Theorem 1.1(a)], and our proof proceeds along similar lines. Note however, that there is a small mistake in the proof of [CGR, Theorem 1.1(a)]. On page 565 in [CGR], in the setting of Lemma 3.2 above, we said that the obstruction $\Delta(a)$ (denoted by $\delta([a])$ there) to lifting a to $H^1(X,S)$ lies in $H^2(X,\mu)$, instead of $H^2(X, {}_a\mu)$. This mistake is corrected in the proof of Lemma 3.2 in the present paper. As a consequence, the (corrected) argument in this paper is a bit longer than in [CGR], and the group S is a bit larger; here $S \cap T = {}_{n^2}T$, where as in [CGR] $S \cap T =_n T$.

5. Toral torsors and a theorem of Grothendieck

Let X be a scheme and G be a smooth affine group scheme over X. Assume that the connected component G^0 is reductive. We say that a G-torsor E over X is *toral* if the twisted X-group scheme ${}^EG$ admits a maximal torus defined over X. We denote by $H^1_{toral}(X,G) \subset H^1(X,G)$ the set of toral classes. The following lemma is well known.

5.1. **Lemma.** *Assume that G^0/X admits a maximal X-torus T. Then*

$$H^1_{toral}(X,G) = \mathrm{Im}\Big(H^1(X,N_G(T)) \to H^1(X,G)\Big).$$

Proof. Let E/X be a G-torsor. The functor $\mathcal{T}/X$ of maximal tori of ${}^EG$ is representable by a separated smooth scheme Σ of finite type over X [SGA3, XII.1.10]. In fact, Σ is the E-twist of homogeneous space $G/N_G(T)$ (whose points represent maximal tori in G); equivalently, Σ can be thought of as the quotient $E/N_G(T)$ (see [SGA3, XXIV.4.2.1]). So the following are equivalent:

(1) ${}^EG$ has a maximal X-torus,

(2) $\mathcal{T}(X) \neq \emptyset$,

(3) $(E/N_G(T))(X) \neq \emptyset$.

By [DG, III, §4, Prop. 4.6], condition (3) is equivalent to

$$[E] \in \mathrm{Im}\Big(H^1(X,N_G(T)) \to H^1(X,G)\Big),$$

and the lemma follows. □

The following theorem of Grothendieck tells us that if G is a reductive group scheme over a semilocal ring k then every G-torsor over k is toral.

5.2. **Theorem.** *(*[SGA3, XIV.3.20]*). Let G be a reductive group scheme defined over a semilocal ring k. Then G admits a maximal k-torus T.* □

The corollary below will be of particular interest to us in the sequel.

5.3. **Corollary.** *Let G be a smooth affine reductive groups scheme defined over a semilocal ring k. Suppose T is a maximal k-torus of G. Then the natural map $H^1(R, N_G(T)) \to H^1(R, G)$ is surjective for any semilocal ring R/k.*

Proof. By Theorem 5.2 every G-torsor over $\mathrm{Spec}(R)$ is toral. That is,

$$H^1(R, G)_{toral} = H^1(R, G)\,.$$

The corollary now follows from Lemma 5.1. □

6. Proof of Theorem 1.2(c)

Throughout this section k will denote a semilocal ring and G an affine connected reductive group scheme defined over k. Suppose that the radical torus of G is isotrivial. We will now proceed to prove Theorem 1.2(c) in four steps.

Case 1. G split, semisimple and adjoint. That is, $G = G_0 \times_{\mathbb{Z}} k$, where G_0 is an adjoint split group defined over $\mathbb{Z}$. Let T_0 be a maximal split torus in G_0 defined over $\mathbb{Z}$ and let $S'_0 \subset N_{G_0}(T_0)$ be the finite subgroup satisfying the conditions of Proposition 3.1 constructed in the previous section. Then $S' = S'_0 \otimes_{\mathbb{Z}} k$ satisfies the same conditions in G, relative to the maximal torus $T = T_0 \otimes_{\mathbb{Z}} k$ of G. The desired conclusion now follows from Proposition 3.1.

Case 2. G is a quasi-split semisimple and adjoint. In this case G is k-isomorphic to the twist ${}_{h_*(a)}(G_1)$, where G_1 is a split adjoint group scheme over k of the same type as G,

$$a \in Z^1_{ét}(k, \mathrm{Aut}_{\mathrm{Dyn}}\,(D))\,,$$

and D is the Dynkin scheme of G_1, relative to a maximal split k-torus $T_1 \subset G_1$; see §2. The cocycle $h_*(a)$ preserves the maximal torus T_1 and the finite subgroup of $N_{G_1}(T_1)$ constructed in Case 1. In Case 1 we called this finite subgroup S'; now we will denote it by S'_1. Recall that S'_1 satisfies the conditions of Proposition 3.1 relative to T_1; that is, S'_1 normalizes T_1 and projects surjectively onto $W_1 = N_{G_1}(T_1)/T_1$. Now observe that the group ${}_{h_*(a)}(S'_1)$ satisfies the same conditions in $G = {}_{h_*(a)}(G_1)$, relative to the maximal k-torus ${}_{h_*(a)}(T_1)$. The desired conclusion now follows from Proposition 3.1.

Case 3: G is semisimple and adjoint. In this case G is a k-twisted form of a Chevalley group G_0 [SGA3, XXIII.5.7]. In other words, there exists a cocycle $b \in Z^1(k, \mathrm{Aut}(G_0))$ such that $G \cong {}_bG_0$. Let a be the image of b under the projection

$$Z^1_{fppf}(k, \mathrm{Aut}(G_0)) \to Z^1_{fppf}(k, \mathrm{Aut}\,(D))\,,$$

where D is the Dynkin scheme of G_0. Consider the following commutative exact diagram of pointed sets

$$\begin{array}{ccccc} & & H^1(k,\,\mathrm{Aut}(G_0)) & \longrightarrow & H^1(k,\,\mathrm{Aut}(D)) \\ & & f_{h_*(a)}\Big\uparrow & & f_a\Big\uparrow \\ H^1(k,\,{}_{h_*(a)}G_0) & \longrightarrow & H^1(k,\,{}_{h_*(a)}\,\mathrm{Aut}(G_0)) & \longrightarrow & H^1(k,\,{}_a\,\mathrm{Aut}(D)) \end{array}$$

where $f_{h_*(a)}$ and f_a stand for the "torsion" bijections; see §2. By a diagram chase, there exists $[c] \in H^1(k,\,{}_{h_*(a)}G_0)$ such that G is isomorphic to the twisted group ${}_c\Big({}_{h_*(a)}G_0\Big)$, i.e., G is a k-inner form of the quasi-split group ${}_{h_*(a)}G_0$.

By Case 2 we know that Theorem 1.2(c) holds for $G_1 = {}_{h_*(a)}G_0$. That is, there exists a maximal torus $T_1 \subset G_1$ defined over k and a finite k-subgroup $S_1 \subset N_G(T_1)$, such that S_1 is an extension of a twisted constant group scheme by a finite k-group of multiplicative type and the natural map $H^1(k, S_1) \longrightarrow H^1(k, N_{G_1}(T_1))$ is surjective. Moreover, by Corollary 5.3 the map $H^1(k, N_{G_1}(T_1)) \to H^1(k, G_1)$ is also surjective. We conclude that the map $H^1(k, S_1) \to H^1(k, G_1)$ is surjective. We may thus assume that c takes values in S_1.

Now set $S := {}_cS_1$. Then S embeds in ${}_cT_1$. Consider the diagram

$$\begin{array}{ccc} H^1(X, S_1) & \xrightarrow{\ \pi_0\ } & H^1(X, N_{G_1}(T_1)) \\ \Big\uparrow & & \Big\uparrow \\ H^1(X, {}_cS_1) & \xrightarrow{\ \pi\ } & H^1(X, N_G({}_cT_1)) \end{array}$$

where the vertical arrows are the "torsion" bijections; see §2. Since π_0 is surjective, so is π.

Case 4. G **is reductive and the radical torus** $C = \mathrm{rad}(G)$ **is isotrivial.**

Consider the adjoint semisimple k-group $H' = G/C(G)$ [SGA3, XXII.4.3] and the coradical torus $C' = \mathrm{corad}(G)$ (*ibid*, XXII.6.2). Informally speaking, C' is the maximal toral quotient of G. Define $G' = H' \times C'$. Then the natural map $G \to G'$ is an isogeny (*ibid*, XXII.6.4); we will denote its kernel by Z.

Since we are assuming that C is an isotrivial k-torus, C' is isotrivial as well (*ibid*, XXIV.4..5) and there exists a finite étale covering $\widetilde{k}/k$ which splits C'. Let m be the degree of the covering $\widetilde{k}/k$ and let μ be the m-torsion subgroup of C'. Note that the canonical mapping $H^1(k, \mu) \to H^1(k, C')$ is surjective. Indeed, the restriction-corestriction formula [CTS, 0.4]

$$\times\, m = \mathrm{Cor}^{\widetilde{k}}_k \circ \mathrm{Res}^{\widetilde{k}}_k :\ H^1(k, C') \to H^1(k, C')$$

together with the fact that $H^1(\widetilde{k}, C') = 0$ (Hilbert's Theorem 90) imply that the map

$$\times\, m\colon H^1(k, C') \to H^1(k, C')$$

is trivial. (Note that this is the same argument we used in Section 3, except that there it was phrased in terms of the trace map.)

Let T' and $S' \subset N_{H'}(T')$ be the subgroups constructed in Case 3 for H' and let X/k be a scheme satisfying condition (1.1). Then the canonical morphism $\pi' : H^1(X, \mu \times S') \to H^1(X, N_{G'}(T'))$ is surjective. We claim that $S = f^{-1}(\mu \times S')$ is as required, i.e. $H^1(X, S) \to H^1(X, N_G(T))$ is surjective where $T = f^{-1}(C' \times T')$.

Indeed, the exact sequences $1 \to Z \to N_G(T) \to N_{G'}(T') \to 1$ and $1 \to Z \to S \to \mu \times S' \to 1$ give rise to a commutative diagram

$$\begin{array}{ccccccc}
H^1(X,Z) & \longrightarrow & H^1(X,N_G(T)) & \xrightarrow{g_1} & H^1(X,N_{G'}(T')) & \xrightarrow{g_2} & H^2(X,Z) \\
\uparrow & & \pi\uparrow & & \pi'\uparrow & & \mathrm{id}\uparrow \\
H^1(X,Z) & \longrightarrow & H^1(X,S) & \xrightarrow{h_1} & H^1(X,\mu\times S') & \xrightarrow{h_2} & H^2(X,Z)
\end{array}$$

Here g_2, h_2 are connecting homomorphisms [Gir, IV.4.3.4]. Fix an element $[a] \in H^1(X, N_G(T))$ and let $[b] = g_1([a])$. Since π' is surjective, there is a class $[c] \in H^1(X, \mu \times S')$ such that $\pi'([c]) = [b]$. Since $h_2([c]) = g_2\pi'([c]) = 0$, there is $[d] \in H^1(X, S)$ such that $h_1([d]) = [c]$. Thus the classes $[a]$ and $\pi([d])$ have the same image in $H^1(X, N_{G'}(T'))$. A twisting argument shows that the map $H^1(X, {}_dZ) \to g_1^{-1}(g_1([a]))$ is surjective; see [Gir, III.3.2.4]. (Note that here ${}_dZ = Z$, because Z is central in G.) Since $Z \subset S$, we have ${}_dZ \subset {}_dS$ implying $[a] \in \operatorname{Im}\pi$. This completes the proof of Theorem 1.2(c). □

7. Proof of Theorem 1.3 and an application

Theorem 1.3 stated in the introduction is an easy consequence of Theorem 1.2(c) and Corollary 5.3. Indeed, choose T and S as in Theorem 1.2(c) and let R be a semilocal ring containing k. Since $X = \operatorname{Spec}(R)$ satisfies condition (1.1), Theorem 1.2(c) tells us that the natural map $H^1(R, S) \to H^1(R, N_G(T))$ is surjective. By Corollary 5.3 the map $H^1(R, N_G(T)) \to H^1(R, G)$ is also surjective, and Theorem 1.3 follows. □

We will now discuss an application of Theorem 1.3. Let G be a linear algebraic group defined over a field k and $\pi\colon Y \to X$ be a G-torsor over a k-scheme X. As usual, we will say that π admits reduction of structure to a k-subgroup $S \subset G$ if the class in $H^1(X, G)$ represented by π lies in the image of the natural map $H^1(X, S) \to H^1(X, G)$. Equivalently, π admits reduction of structure to S if there exists a G-equivariant X-morphism $Y \to G_X/S_X$.

Suppose $U \to X$ is a morphism and Y_U is the pull-back of Y to U:

$$\begin{array}{ccc} Y_U & \longrightarrow & Y \\ {\scriptstyle \pi_U}\downarrow & & {\scriptstyle \pi}\downarrow \\ U & \longrightarrow & X\,. \end{array}$$

We say that Y admits reduction of structure to S *over* U if the G-torsor $\pi_U : Y_U \to U$ admits reduction of structure to S.

7.1. **Proposition.** *Let G be a smooth linear algebraic group defined over a field k. Assume that the connected component G^0 is reductive and either G is connected or k is algebraically closed. Then there exists a finite k-subgroup $S \subset G$, as in Theorem 1.2(1), with the following property. For any G-torsor $\pi: Y \to X$ over an affine k-scheme X and any finite collection of scheme-theoretic points $x_1, \dots, x_n \in X$, there exists an open subscheme $U \subset X$ containing $x_1, \dots, x_n$ such that π admits reduction of structure to S over U.*

Proof. Let $R = \mathcal{O}_{x_1,\dots,x_n}$ be the semilocal ring of X at $x_1, \dots, x_n$. By Theorem 1.3 π admits reduction of structure to a finite subgroup $S \subset G$ over $\mathrm{Spec}(R) \subset X$. That is, there exists a G-equivariant morphism $\phi: Y_R \to G_R/S_R$.

Since R is, by definition, the direct limit of $\mathcal{O}_X(U)$, as U ranges over the open subsets of X containing $x_1, \dots, x_n$, ϕ extends over some open subscheme X_0 of X containing $x_1, \dots, x_n$. In other words, π admits reduction of structure to S over X_0. □

8. Torsors on affine spaces

Let k be a field of characteristic 0, and $\overline{k}$ be an algebraic closure of k. In this section we will apply Theorem 1.2(c) in the case where X is the affine space $\mathbb{A}_k^n$. The key observation here is that $\mathbb{A}_{\overline{k}}^n$ is simply connected. By the fundamental exact sequence for π_1 [SGA1, IX.6.1], we have an isomorphism

$$\pi_1(\mathbb{A}_k^n, \overline{0}) \xrightarrow{\sim} \mathrm{Gal}(\overline{k}/k),$$

where $\pi_1(\mathbb{A}_k^n, \overline{0})$ stands for the algebraic fundamental group of $\mathbb{A}_k^n$ relative to the base point $\overline{0} : \mathrm{Spec}(\overline{k}) \to \mathbb{A}_k^n$. In other words, every finite étale cover of $\mathbb{A}_k^n$ is of the form $\mathbb{A}_K^n$, where K/k is an étale k-algebra. Since $\mathrm{Pic}(\mathbb{A}_K^n) = 0$, this implies that $X = \mathbb{A}_k^n$ satisfies condition (1.1).

8.1. **Proposition.** *Let k be a field of characteristic zero, $n \geq 0$ be an integer, and G be a (connected) reductive group over k. Then*

$$H^1(k, G) \xrightarrow{\sim} H^1(\mathbb{A}_k^n, G)_{toral}.$$

In other words, every toral torsor on $\mathbb{A}_k^n$ is constant.

Proof. Since k is a field, Theorem 1.2(c) applies to G. Let $S \subset G$ be the finite k-subgroup as in Theorem 1.2. As we noted before the statement of the proposition, $X = \mathbb{A}_k^n$ satisfies condition (1.1). Thus the natural map $H^1(\mathbb{A}_k^n, S) \to H^1(\mathbb{A}_k^n, N(T))$ is surjective. By Lemma 5.1, the map

$$H^1(\mathbb{A}_k^n, S) \to H^1(\mathbb{A}_k^n, G)_{toral}$$

is also surjective. The kernel of the natural map $H^1(\mathbb{A}_k^n, S) \to H^1(\mathbb{A}_{\overline{k}}^n, S)$ consists of those S-torsors on $\mathbb{A}_k^n$ which become trivial on $\mathbb{A}_{\overline{k}}^n$. Since $\mathbb{A}_{\overline{k}} \to \mathbb{A}_k$ is a Galois cover, with Galois group $\mathrm{Gal}(\overline{k}/k)$, this kernel is $H^1(k, S(\mathbb{A}_{\overline{k}}^n))$, where H^1 stands for Galois cohomology. Since $S(\mathbb{A}_{\overline{k}}^n) = S(\overline{k})$, this yields an exact sequence

$$1 \to H^1(k, S(\overline{k})) \to H^1(\mathbb{A}_k^n, S) \to H^1(\mathbb{A}_{\overline{k}}^n, S).$$

Since $\mathbb{A}_{\overline{k}}^n$ is simply connected, $H^1(\mathbb{A}_{\overline{k}}^n, S) = 1$, and hence the map

$$H^1(k, S(\overline{k})) \to H^1(\mathbb{A}_k^n, S)$$

is surjective. The commutative exact diagram of pointed sets

$$\begin{array}{ccccc} H^1(k, S(\overline{k})) & \longrightarrow & H^1(\mathbb{A}_k^n, S) & \longrightarrow & 1 \\ \downarrow & & \downarrow & & \\ H^1(k, G) & \longrightarrow & H^1(\mathbb{A}_k^n, G)_{toral} & & \\ \downarrow & & \downarrow & & \\ 1 & & 1 & & \end{array}$$

shows that the natural map $H^1(k, G) \to H^1(\mathbb{A}_k^n, G)_{toral}$ is surjective. This map is also injective. Indeed, suppose G-torsors $T_1 \to \mathrm{Spec}(k)$ and $T_2 \to \mathrm{Spec}(k)$ map to the same G-torsor $Y \to \mathbb{A}_k^n$, i.e., $Y \simeq T_i \times_{\mathrm{Spec}(k)} \mathbb{A}_k^n$ for $i = 1, 2$. Then both T_1 and T_2 are isomorphic to the fiber of Y over $0 \in \mathbb{A}_k^n$. Hence, T_1 and T_2 represent the same class in $H^1(k, G)$. We conclude that the map $H^1(k, G) \to H^1(\mathbb{A}_k^n, G)_{toral}$ is an isomorphism. □

8.2. **Remark.** There are examples of non constant G-torsors P over affine spaces; see Ojanguren-Sridharan [OS] (cf. also [K, VII.10]). Proposition 8.1 tells us that in these examples the twisted groups ${}^P G$ do not carry maximal tori.

8.3. **Remark.** As we pointed out in the introduction, the scheme

$$X = \mathrm{Spec}(k[x_1^{\pm 1}, \ldots, x_n^{\pm 1}])$$

also satisfies condition (1.1) (in characteristic zero), so in this case the map $H^1(X, S) \to H^1(X, G)_{toral}$ is also surjective. This fact is used in [GP].

References

[BT] F. Bruhat, J. Tits, *Groupes réductifs sur un corps local. II. Schémas en groupes. Existence d'une donnée radicielle valuée*, Inst. Hautes Etudes Sci. Publ. Math. **60** (1984), 197–376.

[CGP] V. Chernousov, P. Gille, A. Pianzola, *Torsors on the affine line and on the punctured line*, in preparation.

[CGR] V. Chernousov, P. Gille, Z. Reichstein, *Resolving G-torsors by abelian base extensions*, J. Algebra **296** (2006), 561–581.

[CTS] J.-L. Colliot-Thélène and J.-J. Sansuc, *Principal homogeneous spaces under flasque tori: applications*, J. Algebra **106** (1987), 148–205.

[DG] M. Demazure, P. Gabriel, *Groupes algébriques, I*, North-Holland, 1970.

[GM] P. Gille, L. Moret-Bailly, *Actions algébriques de groupes arithmétiques*, preprint (2006), available on the authors' home pages.

[GP] P. Gille and A. Pianzola, *Galois cohomology and forms of algebras over Laurent polynomial rings II*, in preparation.

[GR] P. Gille and Z. Reichstein, *Lower bounds for the essential dimension of linear algebraic groups*, to appear in Commentarii Math. Helv.

[Gir] J. Giraud, *Cohomologie non-abélienne*, Springer, 1970.

[K] M. A. Knus, *Quadratic and hermitian forms over rings*, Grundlehren der mat. Wissenschaften **294**, Springer, 1991.

[M] J. S. Milne, *Étale Cohomology*, Princeton Mathematical Series, **33**, Princeton University Press, 1980.

[OS] M. Ojanguren, R. Sridharan, *Cancellation of Azumaya algebras*, J. Algebra **18** (1971), 501–505.

[SGA1] *Séminaire de Géométrie algébrique de l'I.H.E.S., Revêtements étales et groupe fondamental, dirigé par A. Grothendieck*, Lecture Notes in Math. 224. Springer, 1971.

[SGA3] *Séminaire de Géométrie algébrique de l'I.H.E.S., 1963-1964, schémas en groupes, dirigé par M. Demazure et A. Grothendieck*, Lecture Notes in Math. 151-153. Springer, 1970.

[SGA4] *Théorie des topos et cohomologie étale des schémas*, Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964, dirigé par M. Artin, A. Grothendieck et J. L. Verdier, Lecture Notes in Math. 269, 270, and 305 (1972), Springer-Verlag.

[Se] J.-P. Serre, *Galois Cohomology*, Springer, 1997.

[T] J. Tits, *Normalisateurs de tores. I. Groupes de Coxeter étendus*, J. Algebra **4** (1966), 96–116.

Department of Mathematics, University of Alberta, Edmonton, Alberta T6G 2G1, Canada
E-mail address: chernous@math.ualberta.ca

UMR 8552 du CNRS, DMA, Ecole normale supérieure, F-75005 Paris, France
E-mail address: Philippe.Gille@ens.fr

Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, Canada
E-mail address: reichst@math.ubc.ca
URL: www.math.ubc.ca/~reichst