Resolving G-torsors by abelian base extensions

V. Chernousov [a,1], P. Gille [b], Z. Reichstein [c,*,2]

[a] *Department of Mathematics, University of Alberta, Edmonton, Alberta T6G 2G1, Canada*
[b] *Laboratoire de mathématiques, Université Paris-Sud, 91405 Orsay, France*
[c] *Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, Canada*

Abstract

Let G be a linear algebraic group defined over a field k. We prove that, under mild assumptions on k and G, there exists a finite k-subgroup S of G such that the natural map $H^1(K, S) \to H^1(K, G)$ is surjective for every field extension K/k. We give several applications of this result in the case where k an algebraically closed field of characteristic zero and K/k is finitely generated. In particular, we prove that for every $\alpha \in H^1(K, G)$ there exists an abelian field extension L/K such that $\alpha_L \in H^1(L, G)$ is represented by a G-torsor over a projective variety. From this we deduce that α_L has trivial fixed point obstruction. We also show that a (strong) variant of the algebraic form of Hilbert's 13th problem implies that the maximal abelian extension of K has cohomological dimension $\leqslant 1$. The last assertion, if true, would prove conjectures of Bogomolov and Königsmann, answer a question of Tits and establish an important case of Serre's Conjecture II for the group E_8.
© 2005 Elsevier Inc. All rights reserved.

Keywords: Linear algebraic group; Torsor; Non-abelian cohomology; G-cover; Unramified cover;
Cohomological dimension; Brauer group; Group action; Fixed point obstruction

* Corresponding author.
 E-mail addresses: chernous@math.ualberta.ca (V. Chernousov), gille@math.u-psud.fr (P. Gille),
reichst@math.ubc.ca (Z. Reichstein).
 URL: http://www.math.ubc.ca/~reichst (Z. Reichstein).

1. Introduction

The starting point for this paper is the following theorem, which will be proved in Sections 2 and 3.

1.1. Theorem. *Let G be a linear algebraic group defined over a field k. Assume that one of the following conditions holds*:

(a) $\mathrm{char}(k) = 0$ *and k is algebraically closed, or*
(b) $\mathrm{char}(k) = 0$ *and G is connected,*
(c) *G is connected and reductive.*

Then there exists a finite k-subgroup S of G, such that the natural map $H^1(K, S) \to H^1(K, G)$ is surjective for every field extension K/k.

Here, as usual $H^1(K, G)$ is the Galois cohomology set $H^1(\mathrm{Gal}(\overline{K}/K), G)$; cf. [Se1]. Recall that this set does not, in general, have a group structure, but has a marked element, corresponding to the trivial (or split) class, which is usually denoted by 1. Given a field extension L/K we will, as usual, denote the image of α under the natural map $H^1(K, G) \to H^1(L, G)$ by α_L.

In the course of the proof of Theorem 1.1 we will construct the finite group S explicitly (see the beginning of Section 2); it is an extension of the Weyl group W of G by a finite abelian group. Moreover, if G is split and k contains certain roots of unity then S can be chosen to be a constant subgroup of G; see Remark 3.1. We also note that Theorem 1.1(a) can be deduced from the results of Bogomolov (see [CS, Lemma 7.3]); we are grateful to J.-L. Colliot-Thélène for pointing this out to us. We will include a self-contained proof of Theorem 1.1(a) in Section 2.

In Section 4 we will discuss Theorem 1.1(a) in the context of invariant theory. In particular, we relate it to a result of Galitskii [Ga] and use it to give a simple proof of the no-name lemma, thus filling a small gap in the existing literature; cf. [CS, Section 4].

Our other applications of Theorem 1.1 are motivated by the following question, implicit in the work of Tits [T2].

1.2. Problem. Let G be a connected algebraic group defined over an algebraically closed field of characteristic zero, K/k be a field extension and $\alpha \in H^1(K, G)$. Is it true that α can always be split by (i) a finite abelian field extension L/K or (ii) by a finite solvable field extension L/K?

Tits [T2, Théorème 2] showed that Problem 1.2(ii) has an affirmative answer for every almost simple group of any type, other than E_8. (He also showed that for every such G, the solvable field extension L/K can be chosen so that each prime factor of $[L : K]$ is a torsion prime of G.) Note that if Problem 1.2(ii) has an affirmative answer for fields K of cohomological dimension $\leqslant 2$, then we would be able to conclude, using an argument originally due to Chernousov, that $H^1(K, E_8) = \{1\}$, thus proving an important (and currently open) case of Serre's Conjecture II; for details, see [PR, Chapter 6] or [Gi, Théorème 11].

We will say that $\alpha \in H^1(K, G)$ is *projective* if it is represented by a torsor over an irreducible complete variety X/k. In other words, $k(X) = K$, and α lies in the image of the natural map $H^1(X, G) \to H^1(K, G)$, restricting a torsor over X to the generic point of X. (Note that after birationally modifying X, we may assume it is smooth and projective.) The split element of $H^1(K, G)$ is clearly projective, and it is natural to think of projective elements of $H^1(K, G)$ as "close" to being split. The following result may thus be viewed as a "first approximation" to the assertion of Problem 1.2.

1.3. Theorem. *Let k be an algebraically closed field of characteristic zero, G/k be a linear algebraic group, K/k be a finitely generated field extension, and $\alpha \in H^1(K, G)$. Then there exists a finite abelian extension L/K, such that α_L is projective.*

Note that the group G in Theorem 1.3 is not assumed to be connected; in particular, the case where G is finite (Proposition 6.1) is key to our proof. On the other hand, in the case where G is connected, Theorem 1.3 does not imply an affirmative answer to Problem 1.2. Indeed, while it is natural to think of α_L as "close to split," it may be not be literally split, even in the case where G is connected and simply connected. To illustrate this point, we will use a theorem of Gabber [CG] to construct a smooth projective 3-fold X/k and a non-trivial class $\alpha \in H^1(k(X), G_2)$ such that α is projective; see Proposition 7.1. (Here G_2 denotes the (split) exceptional group of type G_2 defined over k.)

It is also natural to think of $\alpha \in H^1(K, G)$ as being "close to split" if α has *fixed point obstruction*; for a precise definition, see Section 8. We will show that if α is projective then it has trivial fixed point obstruction; see Proposition 8.1. Combining this result with Proposition 7.1 yields another "approximation" to the assertion of Problem 1.2.

1.4. Corollary. *Let k be an algebraically closed field of characteristic zero, G/k be a linear algebraic group, K/k be a finitely generated field extension, and $\alpha \in H^1(K, G)$. Then there exists a finite abelian extension L/K, such that α_L has trivial fixed point obstruction.*

In Section 9 we will use Theorem 1.1(a) to relate Problem 1.2 to a (strong) variant of Hilbert's 13th problem (Problem 9.3). We will show that if Problem 9.3 had an affirmative answer then so would Problem 1.2 (and, in fact, a much stronger assertion would then hold; see Theorem 9.4 and Remark 9.5).

2. Proof of Theorem 1.1(a)

We begin with the following observation. Let k be a field of characteristic zero, G/k be a linear algebraic group, and $R_u(G)$ be the unipotent radical of G. Recall that G has a Levi decomposition, $G = R_u(G) \rtimes G_{red}$, where G_{red} is a reductive subgroup of G, uniquely determined up to conjugacy. As usual, we shall refer to G_{red} as a *Levi subgroup* of G.

2.1. Lemma. *Let $i : G_{red} \hookrightarrow G$ be a Levi subgroup of G. Then for any field extension K/k, the natural map*

$$i_* : H^1(K, G_{red}) \to H^1(K, G)$$

is a bijection.

Proof. Let $\pi : G \to G/R_{\mathrm{u}}(G)$ be the natural projection. By the Levi decomposition, $G_{\mathrm{red}} \overset{i}{\hookrightarrow} G \overset{\pi}{\to} G/R_{\mathrm{u}}(G)$ is an isomorphism between G_{red} and $G/R_{\mathrm{u}}(G)$. Thus

$$H^1(K, G_{\mathrm{red}}) \overset{i_*}{\longrightarrow} H^1(K, G) \overset{\pi_*}{\longrightarrow} H^1(K, G/R_{\mathrm{u}}(G))$$

is a bijection between $H^1(K, G_{\mathrm{red}})$ and $H^1(K, G/R_{\mathrm{u}}(G))$. By [Sa, Lemma 1.13], π_* is also a bijection. Hence, so is i_*. □

2.2. Remark. Lemma 2.1 tells us that if the natural map

$$H^1(K, S) \to H^1(K, G_{\mathrm{red}})$$

is surjective then so is the natural map

$$H^1(K, S) \to H^1(K, G).$$

In particular, in the course of proving Theorem 1.1(a) and (b) we may replace G by G_{red} and thus assume that G is reductive.

We now proceed with the proof of Theorem 1.1(a). Let k be an algebraically closed field of characteristic zero and G be a linear algebraic group defined over k. As usual, we will identify G with its group of k-points $G(k)$. In view of Remark 2.2, we will assume that G (or equivalently, the connected component G^0 of G) is reductive.

Let T be a maximal torus of G and set $N = N_G(T)$ and $W = N_G(T)/T$. Then W is a finite group and N is an extension of W by T. Let $\mu = {}_nT$ be the group of n-torsion points of T, where $n = |W|$. Consider the exact sequences

$$1 \to T \to N \to W \to 1 \quad \text{and} \quad 1 \to \mu \to T \overset{\times n}{\to} T \to 1.$$

The first sequence yields a class in $H^2(W, T)$. Since $n \cdot H^2(W, T) = 0$, the second sequence tells us that this class comes from $H^2(W, \mu)$. In terms of group extensions, it means that there exists an extension S of W by μ such that N is the push-out of S by the morphism $\mu \hookrightarrow T$. In particular, S is a finite subgroup of N of order $|W|^{\mathrm{rank}(G)+1}$. We will now prove the following variant of Theorem 1.1.

2.3. Proposition. *Assume G is reductive and S is the finite subgroup of G constructed above. Then the map $H^1(K, S) \to H^1(K, G)$ is surjective for any field extension K/k.*

Proof. We claim that the natural map $H^1(K, N) \to H^1(K, G)$ is surjective for every field extension K/k. Indeed, let $\overline{K}$ be an algebraic closure of K. For any $[z] \in H^1(K, G)$ the twisted group ${}_zG^0$ is reductive and has a maximal torus Q. Viewing Q and T as maximal tori in $G^0(\overline{K})$, we see that they are $\overline{K}$-conjugate; the claim now follows from [Se1, Lemma III.2.2.1].

It remains to prove that the map $H^1(K, S) \to H^1(K, N)$ is surjective. We will do this fiberwise, with respect to the map $p_*: H^1(K, N) \to H^1(K, W)$. Let $[a] = p_*([b]) \in H^1(K, W)$. A twisting argument [Se1, I.5.5], shows that the map

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

is surjective; here ${}_bT$ denotes the torus T, twisted by the cocycle b. On the other hand, consider the map $q_*: H^1(K, S) \to H^1(K, W)$ induced by the natural projection $q: S \to W = S/\mu$. Since $H^2(K, \mu) \to H^2(K, T)$ is injective and $\partial([a]) = 0$, where $\partial: H^1(K, W) \to H^2(K, T)$ is the connecting morphism, we conclude that $[a] \in \operatorname{Im} q_*$. It now suffices to prove that the map

$$H^1(K, {}_b\mu) \longrightarrow H^1(K, {}_bT)$$

is surjective. The cokernel of this map is given by the exact sequence

$$H^1(K, {}_b\mu) \longrightarrow H^1(K, {}_bT) \xrightarrow{\times n} H^1(K, {}_bT).$$

The torus ${}_bT$ is split by the Galois extension L/K given by $[a] \in H^1(K, W) = \operatorname{Hom}_{\mathrm{ct}}(\operatorname{Gal}(\overline{K}/K), W)/\operatorname{Int}(W)$, the degree of this extension divides n. The restriction–corestriction formula $\times n = \operatorname{Cor}_k^L \circ \operatorname{Res}_k^L$ and the fact that $H^1(L, T) = 0$ (Hilbert's Theorem 90) imply that the map $\times n: H^1(K, {}_bT) \to H^1(K, {}_bT)$ is trivial. We conclude that the map $H^1(K, {}_b\mu) \to H^1(K, {}_bT)$ is surjective. Hence, the map $H^1(K, S) \to H^1(K, N)$ is surjective as well. $\quad\square$

3. Proof of Theorem 1.1(b) and (c)

In view of Remark 2.2 part (b) follows from part (c). The rest of this section will be devoted to proving part (c). We will consider three cases.

Case 1. Let G be a quasi-split adjoint group. We denote by T a maximal quasi-split torus in G, $N = N_G(T)$ and $W = N_G(T)/T$. For every root $\alpha \in \Sigma = \Sigma(G, T)$, where Σ is the root system of G with respect to T, the corresponding subgroup $G_\alpha \leqslant G$ is isomorphic (over a separable closure of k) to either SL_2 or PSL_2.

Let $T_\alpha = T \cap G_\alpha$ and let $w_\alpha \in N_{G_\alpha}(T_\alpha)$ be a representative of the Weyl group of G_α with respect to the maximal torus T_α given by a matrix

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

By Galois' criteria for rationality, the group L generated by all w_α is k-defined. One easily checks that the intersection $L \cap T$ belongs to the 2-torsion subgroup of T; in particular, L is finite.

Let $\mu = {}_nT$ be the n-torsion subgroup of T where n is the cardinality of the Weyl group W. Consider the subgroup S of N generated by L and μ. Now, arguing as in the proof of Proposition 2.3, and using the fact that T and T/μ are permutation tori (and hence both have trivial Galois cohomology in dimension 1), one checks that the canonical map $H^1(K, S) \to H^1(K, N)$ is surjective for every extension K/k. In the course of the proof of Proposition 2.3 we showed that $H^1(K, N) \to H^1(K, G)$ is surjective. Then the composite map $H^1(K, S) \to H^1(K, N) \to H^1(K, G)$ is surjective as well.

Case 2. Let G be an adjoint k-group. Denote by G_0 the quasi-split adjoint group of the same inner type as G. One knows (see [T1]) that $G = {}_a(G_0)$ is the twisted form of G_0 for an appropriate cocycle $a \in Z^1(k, G_0)$. If S_0 is the subgroup of G_0 constructed in Case 1, we may assume without loss of generality that a takes values in S_0. Let $S = {}_aS_0$ and consider the diagram

$$
\begin{array}{ccc}
H^1(K, S_0) & \xrightarrow{\pi_0} & H^1(K, G_0) \\
\uparrow{\scriptstyle f_S} & & \uparrow{\scriptstyle f_G} \\
H^1(K, S) & \xrightarrow{\pi} & H^1(K, G).
\end{array}
$$

Here f_S and f_G are natural bijections. Since π_0 is surjective, so is π.

Case 3. Let G be a connected reductive k-group. It is an almost direct product of the semisimple k-group $H = [G, G]$ and the central k-torus C of G. Let Z be the center of H. Clearly, we have $C \cap H \leqslant Z$. Consider the group $G' = G/Z$ and a natural morphism $f : G \to G'$. By our construction, G' is the direct product of the torus $C/C \cap H$ and the adjoint group $H' = H/Z$.

Let S' be the subgroup constructed in Case 2 for H' and let $\mu = {}_n(C/C \cap H)$ be the n-torsion subgroup of the torus $C/C \cap H$, where n is the degree of the minimal extension of k splitting C. Then for any extension K/k a natural morphism $H^1(K, \mu \times S') \to H^1(K, G')$ is surjective. We claim that $S = f^{-1}(\mu \times S')$ is as required, i.e., $H^1(K, S) \to H^1(K, G)$ is surjective.

Indeed, the exact sequences $1 \to Z \to G \to G' \to 1$ and $1 \to Z \to S \to S' \to 1$ give rise to a commutative diagram

$$
\begin{array}{ccccccc}
H^1(K, Z) & \longrightarrow & H^1(K, G) & \xrightarrow{g_1} & H^1(K, G') & \xrightarrow{g_2} & H^2(K, Z) \\
\uparrow & & \uparrow{\scriptstyle \pi} & & \uparrow{\scriptstyle \pi'} & & \uparrow{\scriptstyle id} \\
H^1(K, Z) & \longrightarrow & H^1(K, S) & \xrightarrow{h_1} & H^1(K, \mu \times S') & \xrightarrow{h_2} & H^2(K, Z)
\end{array}
$$

Here g_2, h_2 are connecting homomorphisms. Let $[a] \in H^1(K, G)$ and $[b] = g_1([a])$. Since π' is surjective, there is a class $[c] \in H^1(\mu \times S')$ such that $\pi'([c]) = [b]$. Since $h_2([c]) =$

$g_2\pi'([c]) = 0$, there is $[d] \in H^1(K, S)$ such that $h_1([d]) = [c]$. Thus two classes $[a]$ and $\pi([d])$ have the same image in $H^1(K, G')$. By a twisting argument, one gets a surjective map $H^1(K, {}_dZ) \to g^{-1}(g_1([a]))$. Since $Z \subset S$ and hence ${}_dZ \subset {}_dS$, we have $[a] \in \operatorname{Im} \pi$. This completes the proof of Theorem 1.1.

3.1. Remark. Our argument shows that if G is split and k contains certain roots of unity, then the subgroup S in parts (b) and (c) can be taken to be a constant group.

More precisely, in part (c), k needs to have a primitive root of unity of degree $n = |W(G_{\mathrm{ss}})| \cdot |Z(G_{\mathrm{ss}})|$, where $W(G_{\mathrm{ss}})$ and $Z(G_{\mathrm{ss}})$ denote, respectively, the Weyl group and the center of the semisimple part G_{ss} of G.

The same is true in part (b), except that G needs to be replaced by $G_{\mathrm{red}} = G/R_{\mathrm{u}}(G)$ in the above definition of n.

4. Theorem 1.1 in the context of invariant theory

For the rest of this paper k will be an algebraically closed field of characteristic zero, K will be a finitely generated extension of k and G will be a linear algebraic group defined over k. In this section we will introduce some terminology in this context, discuss an invariant-theoretic interpretation of Theorem 1.1(a) and use it to give a simple proof of the no-name lemma. The third author would like to thank V.L. Popov for helpful suggestions concerning this material.

4.1. (G, S)-sections

Recall that every element of $H^1(K, G)$ is uniquely represented by a primitive generically free G-*variety* V, up to birational isomorphism. That is, $k(V)^G = K$, the rational quotient map $\pi : V \dashrightarrow V/G$ is a torsor over the generic point of V/G, and this torsor is α; see [Po, 1.3]. (Here "V is primitive" means that G transitively permutes the irreducible components of V. In particular, if G is connected then V is irreducible.)

If S is a closed subgroup of G and $\alpha \in H^1(K, S)$ is represented by a generically free S-variety V_0, then the image of α in $H^1(K, G)$ is represented by the G-variety $G *_S V_0$, which is, by definition, the rational quotient of $G \times V_0$ for the S-action given by $s : (g, v_0) \mapsto (gs^{-1}, s \cdot v_0)$. We shall denote the image of (g, v_0) in this quotient by $[g, v_0]$. Note that a rational quotient is, a priori, only defined up to birational isomorphism; however, a regular model for $G *_S V_0$ can be chosen so that the G-action on $G \times V_0$ (by translations on the first factor) descends to a regular G-action on $G *_S V_0$, making the rational quotient map $G \times V_0 \dashrightarrow G *_S V_0$ G-equivariant (via $g' \cdot [g, v_0] \mapsto [g'g, v_0]$); see [Re, 2.12]. If S is a finite group and V_0 is a quasi-projective S-variety (which will be the case in the sequel) then we may take $G *_S V_0$ to be the geometric quotient for the S-action on $G \times V_0$, as in [PV, Section 4.8].

Now let V be a G-variety. An S-invariant subvariety $V_0 \subset V$ is called a (G, S)-*section* if

(a) $G \cdot V_0$ is dense in V and
(b) V_0 has a dense open S-invariant subvariety U such that $g \cdot u \in V_0$ for some $u \in U$ implies $g \in S$.

The above definition is due to Katsylo [Ka]; sometimes a (G, S)-section is also called a *standard relative section* (see [Po, 1.7.6]) or *a relative section* with normalizer S (see [PV, Section 2.8]). A G-variety V is birationally isomorphic to $G *_S V_0$ for some S-variety V_0 if and only if V has a (G, S)-section; see [PV, Section 2.8]. In this context Theorem 1.1(a) can be rephrased as follows:

Theorem 1.1′. *Every generically free G-variety has a (G, S)-section, where S is a finite subgroup of G.*

Recall that a subvariety V_0 of a generically free G-variety V is called a *Galois quasisection* if the rational quotient map $\pi : V \dashrightarrow V/G$ restricts to a dominant map $V_0 \dashrightarrow V/G$, and the induced field extension $k(V_0)/k(V)^G$ is Galois. If V_0 is a Galois quasisection then the finite group $\Gamma(V_0) := \mathrm{Gal}(k(V_0)/k(V)^G)$ is called the Galois group of V_0; see [Ga] or [Po, (1.1.1)]. (Note $\Gamma(V_0)$ is not required to be related to G in any way.) The following theorem is due to Galitskii [Ga]; cf. also [Po, (1.6.2) and (1.17.6)].

4.2. Theorem. *If G is connected then every generically free G-variety has a Galois quasisection.*

A (G, S)-section is clearly a Galois quasisection with Galois group S. Hence, Theorem 1.1′ (or equivalently, Theorem 1.1(a)) may be viewed as an extension of Theorem 4.2. Note that the Galois group $\Gamma(V_0)$ of the Galois quasisection V_0 constructed in the proof of Theorem 4.2 is isomorphic to a subgroup of the Weyl group $W(G)$; cf. [Po, Remark 1.6.3]. On the other hand, the group S in our proof of Theorem 1.1(a), is an extension of $W(G)$ by a finite abelian group. Enlarging the finite group S may thus be viewed as "the price to be paid" for a section with better properties.

4.3. The no-name lemma

A G-bundle $\pi : V \to X$ is an algebraic vector bundle with a G-action on V and X such that π is G-equivariant and g restricts to a linear map $\pi^{-1}(x) \to \pi^{-1}(gx)$ for every $x \in X$.

4.4. Lemma (No-name lemma). *Let $\pi : V \to X$ be a G-bundle of rank r. Assume that the G-action on X is generically free. Then there exists a birational isomorphism $\pi : V \overset{\sim}{\dashrightarrow} X \times \mathbb{A}^r$ of G-varieties such that the following diagram commutes*

$$
\begin{array}{ccc}
V & \overset{\phi}{\dashrightarrow} & X \times \mathbb{A}^r \\
\ \ \downarrow{\scriptstyle \pi} & \swarrow{\scriptstyle \mathrm{pr}_1} & \\
X & &
\end{array}
\tag{4.5}
$$

Here G is assumed to act trivially on $\mathbb{A}^r$, and pr_1 denotes the projection to the first factor. In particular, $k(V)^G$ is rational over $k(X)^G$.

The term "no-name lemma," due to Dolgachev [Do], reflects the fact that this result was independently discovered by many researchers. In the case where G is a finite group,

Lemma 4.4 (otherwise known as Speiser's lemma, see [Sp]) may be viewed as a restatement of Hilbert's Theorem 90. In this case there are many proofs in the literature; see, e.g., [EM, Proposition 1.1], [L, Proposition 1.3], [Sh, Appendix 3] or [CS, Section 4]. For algebraic groups G Lemma 4.4 was noticed more recently (the earliest reference we know is [BK]). This fact is now widely known and much used; however, as Colliot-Thélène and Sansuc observed in [CS, Section 4], a detailed proof has never been published. We will now use Theorem 1.1(a) (or equivalently, Theorem 1.1$'$ above) to give a simple argument reducing the general case of the no-name lemma to the case of a finite group.

Proof of the no-name lemma. By Theorem 1.1$'$ X has a (G, S)-section X_0 for some finite subgroup S of G. Then $V_0 = \pi^{-1}(X_0)$ is a (G, S)-section for V; cf. [Po, (1.7.7), Corollary 2]. In other words, $X \simeq X_0 *_S G$ and $V \simeq V_0 *_S G$, where $\simeq$ denotes birational isomorphism of G-varieties.

Note that V_0 is an S-vector bundle over X_0. Since we know that the no-name lemma holds for S, there is an S-equivariant birational isomorphism $\phi_0 : V_0 \xdashrightarrow{\sim} X_0 \times \mathbb{A}^r$ such that the diagram of S-varieties

$$
\begin{array}{ccc}
V_0 & \xdashrightarrow{\ \phi_0\ } & X_0 \times \mathbb{A}^r \\
\ \downarrow{\scriptstyle \pi} & \swarrow{\scriptstyle \mathrm{pr}_1} & \\
X_0 & &
\end{array}
\tag{4.6}
$$

commutes. Taking the homogeneous fiber product of this diagram with G, we obtain

$$
\begin{array}{ccc}
V \simeq V_0 *_S G & \xdashrightarrow{\ \phi\ } & \left(X_0 \times \mathbb{A}^r\right) *_S G \simeq X \times \mathbb{A}^r \\
\ \downarrow{\scriptstyle \pi} & \swarrow{\scriptstyle \mathrm{pr}_1} & \\
X \simeq X_0 *_S G, & &
\end{array}
$$

where $\phi = \phi_0 *_S G$. $\square$

4.7. Remark. The above argument can be naturally rephrased in cohomological terms. Let $K = k(X)^G = k(X_0)^S$. Then Lemma 4.4 is equivalent to the following assertions: (i) $k(V)^G = K(t_1, \ldots, t_r)$ and (ii) α_V is the image of α_X under the restriction map $H^1(K, G) \to H^1(K(t_1, \ldots, t_r), G)$.

Diagram (4.6) tells us that (i)$'$ $k(V_0)^S = K(t_1, \ldots, t_r)$ and (ii)$'$ α_{V_0} is the image of α_{X_0} under the natural map $H^1(K, S) \to H^1(K(t_1, \ldots, t_r), S)$. (i) follows immediately from (i)$'$, and (ii) follows from (ii)$'$ by considering the natural diagram

$$
\begin{array}{ccc}
\alpha_{X_0} \in H^1(K, S) & \longrightarrow & H^1\big(K(t_1, \ldots, t_r), S\big) \ni \alpha_{V_0} \\
\ \downarrow{\scriptstyle \mathrm{res}} & & \ \downarrow{\scriptstyle \mathrm{res}} \\
\alpha_X \in H^1(K, G) & \longrightarrow & H^1\big(K(t_1, \ldots, t_r), G\big) \ni \alpha_V.
\end{array}
$$

5. Preliminaries on *G*-covers

Let G be a finite group. We shall call a finite morphism $\pi : X' \to X$ of algebraic varieties a *G-cover*, if X is irreducible, G acts on X', so that π maps every G-orbit in X' to a single point in X, and π is a G-torsor over a dense open subset U of X. We will express the last condition by saying that π is *unramified* over U. Restricting π to the generic point of X, we obtain a torsor $\alpha \in H^1(k(X), G)$ over $\operatorname{Spec} k(X)$. In this situation we shall say that π represents α. If a cover $\pi : X' \to X$ is unramified over all of X, then we will simply say that π is *unramified*.

Recall that $\alpha \in H^1(K, G)$ is called *unramified* if it lies in the image of $H^1(R, G) \to H^1(K, G)$ for every discrete valuation ring $k \subset R \subset K$ and *projective*, if it is represented by an unramified G-cover $\pi : X' \to X$ over a complete (or equivalently, projective) variety X.

5.1. Lemma. *Let G be a finite group, K be a finitely generated extension of an algebraically closed base field k of characteristic zero, and $\alpha \in H^1(K, G)$. Then the following assertions are equivalent*:

(a) *α is represented by a projective G-variety V (in the sense of Section 4), such that every element $1 \neq g \in G$ acts on V without fixed points,*
(b) *α is projective, and*
(c) *α is unramified.*

Note that condition (b) can be rephrased by saying that α has trivial fixed point obstruction; see Section 8.

Proof. (a) $\Rightarrow$ (b). The G-action on V has a geometric quotient $\pi : V \to X$, where X is a projective variety; cf., e.g., [PV, Section 4.6]. We claim that π is a torsor over X. Indeed, we can cover V by G-invariant affine open subsets V_i. The quotient variety X is then covered by affine open subsets $X_i = \pi(V_i)$, moreover, $\pi_i = \pi_{|V_i} : V_i \to X_i$ is the geometric quotient for the G-action on V_i; see [PV, Theorem 4.16]. It is thus enough to show that $\pi_i : V_i \to X_i$ is a torsor for each i. This is an immediate corollary of the Luna Slice Theorem; see, e.g., [PV, Theorem 6.1].

(b) $\Rightarrow$ (c). Suppose α is represented by a G-torsor $V \to X$, where X is a projective variety with $k(X) = K$. We want to prove that for any discrete valuation ring $R \subset K$ the class α belongs to the image $H^1(R, G) \to H^1(K, G)$.

Indeed, the ring R dominates a point in X; denote this point by D. Consider the canonical map $\operatorname{Spec} R \to X$ sending the closed point in $\operatorname{Spec} R$ to D and the generic point of $\operatorname{Spec} R$ into the generic point of X. Take the fiber product $(\operatorname{Spec} R) \times_X V$. It follows immediately from this construction that the G-torsor

$$(\operatorname{Spec} R) \times_X V \to \operatorname{Spec} R$$

is as required, i.e., its image under the map $H^1(R, G) \to H^1(K, G)$ is α.

(c) $\Rightarrow$ (a). Let V be a smooth projective G-variety representing α and let $\pi : V \to X$ be the geometric quotient. Note that X is normal. We want to show that every $1 \neq g \in G$ acts on V without fixed points. Assume the contrary: $gv = v$ for some $v \in V$. By [RY2, Theorem 9.3] (with $s = 1$ and $H_1 = \langle g \rangle$), after performing a sequence of blowups with smooth G-invariant centers on V, we may assume that the fixed point locus V^g of g contains a divisor $D \subset V$. If $R = \mathcal{O}_{X, \pi(D)}$ is the local ring of the divisor $\pi(D)$ in X then α does not lie in the image of the natural morphism $H^1(R, G) \to H^1(K, G)$, a contradiction. $\quad\square$

5.2. Remark. Our proof of the implication (b) $\Rightarrow$ (c) does not use the fact that G is a finite group. This implication is valid for every linear algebraic group G.

6. Proof of Theorem 1.3

Let S be the finite subgroup of G given by Theorem 1.1(a). Then $\alpha \in H^1(K, G)$ is the image of some $\beta \in H^1(K, S)$. Examining the diagram

$$
\begin{array}{ccc}
H^1(X, S) & \longrightarrow & H^1(L, S) \ni \beta_L \\
\downarrow & & \downarrow \\
H^1(X, G) & \longrightarrow & H^1(L, G) \ni \alpha_L,
\end{array}
$$

where X is a complete variety and $L = k(X)$, we see that if Theorem 1.3 holds for S then it holds for G.

From now on we may assume that G is a finite group. In this case Theorem 1.3 can be restated as follows.

6.1. Proposition. *Let G be a finite group, k be an algebraically closed base field of characteristic zero, K/k be a finitely generated extension, and $\alpha \in H^1(K, G)$. Then there exists an abelian field extension L/K such that α_L is represented by an unramified G-cover $\pi : Z' \to Z$, where Z and Z' are projective varieties.*

The rest of this section will be devoted to proving Proposition 6.1. We begin with the following lemma.

6.2. Lemma. *Let G be a finite group. Then every $\alpha \in H^1(K, G)$ is represented by a G-cover $\pi : X' \to X$ such that*

(a) *X' is normal and projective,*
(b) *X is smooth and projective,*
(c) *there exists a normal crossing divisor D on X such that π is unramified over $X - D$.*

Proof. Suppose α is represented by a G-Galois algebra K'/K. We may assume without loss of generality that K' is a field. Indeed, otherwise α is the image of some

$\alpha_0 \in H^1(K, G_0)$, where G_0 is a proper subgroup of G, and we can replace G by G_0 and α by α_0.

Choose a smooth projective model Y/k for K/k and let $\phi : Y' \to Y$ be the normalization of Y in K'. Then Y' is projective (see [Mu, Theorem III.8.4, p. 280]), and by uniqueness of normalization (see [Mu, Theorem III.8.3, pp. 277–278]), G acts on Y' by regular morphisms, so that $k(Y')$ is isomorphic to K' as a G-field (see [Mu, pp. 277–278]). We have thus shown that α can be represented by a cover $\phi : Y' \to Y$ satisfying conditions (a) and (b). We will now birationally modify this cover to obtain another cover $\pi : X' \to X$ which satisfies condition (c) as well.

The cover ϕ is unramified over a dense open subset of Y; denote this subset by U. Set $E = Y - U$, and resolve E to a normal crossing divisor D via a birational morphism $\gamma : X \to Y$. Now consider the diagram

$$
\begin{array}{ccc}
X' & \longrightarrow & Y' \\
\downarrow {\scriptstyle \pi} & & \downarrow {\scriptstyle \phi} \\
X & \xrightarrow{\ \gamma\ } & Y,
\end{array}
$$

where X' is the normalization of X in K'. By our construction X is smooth and X' is normal. Moreover, since γ is an isomorphism over U, π is unramified over $X - D = \phi^{-1}(U)$, as desired. $\quad\square$

We are now ready to complete the proof of Proposition 6.1. Our argument will be based on [GM, Theorem 2.3.2], otherwise known as "Abhyankar's lemma," which describes the local structure of a covering, satisfying conditions (a)–(c) of Lemma 6.2, in the étale topology. We thank K. Karu for bringing this result to our attention.

Let $\pi : X' \to X$ be a G-cover of projective varieties representing α and satisfying conditions (a)–(c) of Lemma 6.2. Denote the irreducible components of D by $D_1, \dots, D_s$.

Since X is smooth, each $x \in X$ has an affine open neighborhood U_x where each D_j is principal, i.e., is given by $\{a_{x,j} = 0\}$ for some $a_{x,j} \in \mathcal{O}_X(U_x)$ (possibly $a_{x,j} = 1$ for some x and j). By quasi-compactness, finitely many of these open subsets, say, $U_{x_1}, \dots, U_{x_n}$ cover X. To simplify our notation, we set $U_i = U_{x_i}$ and $a_{ij} = a_{x_i, j}$.

Now let b_{ij} be an $|G|$th root of a_{ij} in the algebraic closure of $K = k(X)$ and $L = K(b_{ij})$, where i ranges from 1 to n and j ranges from 1 to s. Suppose $\gamma : Z \to X$ is the normalization of X in L and $Z' = X' \times_X Z$. Since we are assuming that k is algebraically closed of characteristic zero (and in particular, k contains a primitive $|G|$th root of unity), L/K is an abelian extension. It is also easy to see from our construction that Z and Z' are projective, Z is normal, and the natural projection $\pi' : Z' \to Z$ is a G-cover, which represents $\alpha_L \in H^1(L, G)$. To sum up, we have constructed the following diagram of morphisms:

$$
\begin{array}{ccc}
Z' & \longrightarrow & X' \\
\downarrow {\scriptstyle \psi} & & \downarrow {\scriptstyle \pi} \\
Z & \xrightarrow{\ \gamma\ } & X.
\end{array}
$$

It remains to show that the G-cover ψ is unramified. Suppose we want to show that ψ is unramified at $z_0 \in Z$. Since the open sets $U_1, \ldots, U_n$ cover X, $x_0 = \gamma(z_0)$ lies in U_i for some $i = 1, \ldots, n$. By Abhyankar's lemma [GM, Theorem 2.3.2], there exists an abelian subgroup $H \simeq \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_s\mathbb{Z}$ of G (possibly with $n_j = 1$ for some j) and a (Kummer) H-Galois cover

$$V_i = \left\{ (x, t_1, \ldots, t_s) \mid t_1^{n_1} = a_{i,1}, \ldots, t_s^{n_s} = a_{i,s} \right\} \subset U_i \times \mathbb{A}^s,$$

such that the G-covers $\pi : X' \to X$ and $\phi : G *_H V_i \to U_i$ are isomorphic over an étale neighborhood of x_0 in X. (Here the natural projection $V_i \to U_i$ is an H-cover, $G *_H V_i \to U_i$ is the G-cover induced from it; for a definition of $G *_H V_i$, see Section 4.)

Now recall that by our construction the elements $b_{ij} \in L = k(Z)$ satisfy $b_{ij}^{|G|} = a_{ij} \in \mathcal{O}_X(U_i)$. In particular, they are integral over U_i and thus they are regular function on $\gamma^{-1}(U_i)$. Since n_j divides $|G|$ for every $j = 1, \ldots, s$, the pull-back of ϕ to Z splits over an étale neighborhood of z_0; hence, so does $\psi =$ pull-back of π. In other words, ψ is unramified at z_0, as claimed. This completes the proof of Proposition 6.1. $\quad\square$

7. An example

It is well known that there exist non-trivial projective elements in $H^1(K, \mathrm{PGL}_n)$ for every $n \geqslant 2$ (for suitable K). In this section we use a variant of a construction of Colliot-Thélène and Gabber [CG] to show that, for certain K, such elements exist in $H^1(K, G_2)$ as well.

7.1. Proposition. *Let k be an algebraically closed base field of characteristic zero such that* $\mathrm{trdeg}_{\mathbb{Q}}(k) \geqslant 3$. (*Note that the last condition is satisfied by every uncountable field.*) *Then there exist a smooth projective 3-fold X/k with function field $K = k(X)$ and a projective non-trivial class $\alpha \in H^1(K, G_2)$.*

Note that no such examples can exist if X is a curve or a surface, since in this case $H^1(k(X), G_2) = \{1\}$; see [BP].

Proof. Let E_1, E_2, E_3 be elliptic curves. For $i = 1, 2, 3$ choose $p_i, q_i \in E_i$ so that $p_i \ominus q_i$ is a point of order 2. (Here $\ominus$ denotes subtraction with respect to the group operation on E_i.) Then $2p_i - 2q_i$ is a principal divisor on E_i and $p_i - q_i$ is not; see, e.g., [Si, Corollary 3.5]. Thus $2p_i - 2q_i = \mathrm{div}(f_i)$, where $f_i \neq 0$ is a rational function on E_i, which is not a complete square. Adjoining $\sqrt{f_i}$ to $k(E_i)$, we obtain an irreducible unramified $\mathbb{Z}/2\mathbb{Z}$-cover $\pi_i : E_i' \to E_i$. (Note that by the Hurwitz formula, E_i' is also an elliptic curve.)

Now set $X = E_1 \times E_2 \times E_3$ and $K = k(X)$, $S = (\mathbb{Z}/2\mathbb{Z})^3$, and consider the element $\beta \in H^1(k(X), S)$, represented by the S-cover

$$\pi = (\pi_1, \pi_2, \pi_3) : E_1' \times E_2' \times E_3' \longrightarrow E_1 \times E_2 \times E_3 = X.$$

Since π is an unramified cover, β is projective.

We now recall that the exceptional group G_2/k contains a unique (up to conjugacy) maximal elementary abelian 2-group $i : S = (\mathbb{Z}/2\mathbb{Z})^3 \hookrightarrow G_2$. Set $\alpha = i_*(\beta) \in H^1(K, G_2)$. Since β is projective, so is α. It thus remains to show that $\alpha \neq 1$ in $H^1(K, G_2)$ (for a suitable choice of E_i and E_i').

The cohomology set $H^1(K, G_2)$ classifies octonion algebras or equivalently, 3-fold Pfister forms; cf. [Se2, Theorem 9]. By [GMS, Section 22.10], the map

$$H^1(K, S) = \left(K^\times/(K^\times)^2\right)^3 \xrightarrow{\ i_* \ } H^1(K, G_2)$$

is non-trivial; hence, it sends $(a_1, a_2, a_3) \in (K^\times/(K^\times)^2)^3$ to the class of the 3-Pfister form $\langle\langle a_1, a_2, a_3 \rangle\rangle$; see [GMS, Theorem 27.15]. By our construction, $\beta \in H^1(K, S)$ corresponds to $(f_1, f_2, f_3) \in (K^\times/(K^\times)^2)^3$. Thus $\alpha = i_*(\beta)$ is non-split in $H^1(K, G_2)$ if and only if the 3-fold Pfister form $\langle\langle f_1, f_2, f_3 \rangle\rangle$ is nonsplit or, equivalently, if $(f_1) \cup (f_2) \cup (f_3) \neq 0$ in $H^3(k(X), \mathbb{Z}/2\mathbb{Z})$; see [EL, Corollary 3.3].

Since we are assuming that $\operatorname{trdeg}_{\mathbb{Q}}(k) \geqslant 3$, we can choose elliptic curves E_1, E_2 and E_3 so that their j-invariants are algebraically independent over $\mathbb{Q}$. We now appeal to a theorem of Gabber ([CG, p. 144]), which says that $(f_1) \cup (f_2) \cup (f_3) \neq 0$ in $H^3(k(X), \mathbb{Z}/2\mathbb{Z})$. Hence, $\alpha \neq 1$ in $H^1(K, G)$, as claimed. This completes the proof of Proposition 7.1. $\square$

8. The fixed point obstruction

We now recall the notion of *fixed point obstruction* from [RY3, Introduction]. Suppose $\alpha \in H^1(K, G)$ is represented by a generically free primitive G-variety V (as in Section 4). We shall say that a subgroup of G is *toral* if it lies in a subtorus of G and *non-toral* otherwise. If V (or any G-variety birationally isomorphic to it) has a smooth point fixed by a non-toral diagonalizable subgroup $H \subset G$, then we shall say that V (or equivalently, α) has *non-trivial fixed point obstruction*; cf. [RY3, Introduction]. Note that after birationally modifying V, we may assume that V is smooth and complete (or even projective, see, e.g., [RY2, Proposition 2.2]), and that the fixed point obstruction can be detected on any such model. In other words, if V and V' are smooth complete birationally isomorphic G-varieties then $V^H = \emptyset$ if and only if $(V')^H = \emptyset$ for any diagonalizable subgroup $H \subset G$; see [RY1, Proposition A2]. If $V^H = \emptyset$ for every diagonalizable non-toral subgroup $H \subset G$ (and V is smooth and complete), then we will say that V, or equivalently α, has *trivial fixed point obstruction*.

If α is split (i.e., $\alpha = 1$ in $H^1(K, G)$) then by [RY2, Lemma 4.3] α has trivial fixed point obstruction. We will now extend this result as follows.

8.1. Proposition. *If $\alpha \in H^1(K, G)$ is projective then α has trivial fixed point obstruction.*

Proof. Let $\overline{G}$ be a smooth projective $G \times G$-variety, which contains G as a dense open orbit. (Here we are viewing G as a $G \times G$-variety with respect to left and right multiplication.) To construct $\overline{G}$, we use a theorem of Kambayashi, which says that G can be $G \times G$-equivariantly embedded into $\mathbb{P}(V)$ for some linear representation $G \times G \to \mathrm{GL}(V)$;

see [PV, Theorem 1.7]. Taking the closure of G in $\mathbb{P}(V)$, and $G \times G$-equivariantly resolving its singularities, we obtain $\overline{G}$ with desired properties.

For $\overline{g} \in \overline{G}$, we will write $g_1 \cdot \overline{g} \cdot g_2^{-1}$ instead of $(g_1, g_2) \cdot \overline{g}$; the reason for this notation is that for $\overline{g} \in G$, $(g_1, g_2) \cdot \overline{g} = g_1 \overline{g} g_2^{-1} \in G$.

Since α is projective, it can be represented by a G-torsor $\pi : Z \to X$ over a smooth projective irreducible variety X. (Here $K = k(X)$.) We will now construct a smooth complete G-variety $\overline{Z}$ representing α (i.e., birationally isomorphic to Z) by "enlarging" each fiber of π from G to $\overline{G}$.

Let $U_i \to X$, $i \in I$ be an étale covering which trivializes π. Then π is described by the transition maps $f_{ij} : U_{ij} \times G \to U_{ij} \times G$ on the pairwise "overlaps" U_{ij}; here each f_{ij} is an automorphism of the trivial G-torsor $U_{ij} \times G$ on U_{ij}. (G acts trivially on U_{ij} and by left translations on itself.) These transition maps satisfy a cocycle condition (for Cech cohomology) which expresses the fact that they are compatible on triple "overlaps" U_{hij}. It is easy to see that f_{ij} is given by the formula

$$f_{ij}(u, g) = \big(u, g \cdot h_{ij}(u)\big), \tag{8.2}$$

for some morphism $h_{ij} : U_{ij} \to G$. (In fact, $h_{ij}(u) = \mathrm{pr}_2 \circ f_{ij}(u, 1_G)$, where $\mathrm{pr}_2 : U_{ij} \times G \to G$ is the projection to the second factor.) Formula (8.2) can now be used to extend f_{ij} to a G-equivariant automorphism

$$\overline{f_{ij}} : U_{ij} \times \overline{G} \longrightarrow U_{ij} \times \overline{G},$$

where G acts on $\overline{G}$ on the left. Since f_{ij} satisfies the cocycle condition and G is dense in $\overline{G}$, we conclude that $\overline{f_{ij}}$ satisfy the cocycle condition as well. By descent theory, the transition maps $\overline{f_{ij}}$ patch together to yield a variety $\overline{Z}$ and a commutative diagram of morphisms

$$
\begin{array}{ccc}
Z & \lhook\joinrel\longrightarrow & \overline{Z} \\
& \searrow^{\pi} \quad \swarrow_{\bar{\pi}} & \\
& X &
\end{array}
$$

which locally (in the étale topology) looks like

$$
\begin{array}{ccc}
U_i \times G & \lhook\joinrel\longrightarrow & U_i \times \overline{G} \\
& \searrow^{\pi} \quad \swarrow_{\bar{\pi}} & \\
& U_i &
\end{array}
$$

(The maps π and $\overline{\pi}$ in the second diagram are projections to the first component.) It is now easy to see that $\overline{Z}$ is smooth and proper over X and $Z \hookrightarrow \overline{Z}$ is a G-equivariant open embedding. Indeed, these properties can be checked locally (in the étale topology) on X, where they are immediate from the second diagram. Note also that since $\overline{Z}$ is proper over X, and X is projective over k, $\overline{Z}$ is complete as a k-variety.

Having constructed a smooth complete model $\overline{Z}$ for α, we are now ready to show that α has trivial fixed point obstruction. Suppose a diagonalizable subgroup H of G has a fixed point in $z \in \overline{Z}$. We want to show that H is toral in G. Indeed, let F be the fiber of $\overline{\pi}$ containing z. By our construction $F \simeq \overline{G}$ as G-varieties (here $\overline{G}$ is viewed as a G-variety with respect to the left G-action). We conclude that H has a fixed point in $\overline{G}$. Since $\overline{G}$ has G as a G-invariant dense open subset, it is split as a G-variety (i.e., it represents the trivial class in $H^1(k, G)$), [RY2, Lemma 4.3] now tells us that H is toral. This shows that α has trivial fixed point obstruction, thus completing the proof of Proposition 8.1. $\square$

8.3. Remark. The fact that G acts on $\overline{G}$ both on the right and on the left was crucial in the construction of $\overline{Z}$ in the above proof. The action on the right was used to glue the transition maps $\overline{f_{i,j}}$ together, and the action on the left to define a G-action on $\overline{Z}$. If G could only act on $\overline{G}$ on one side, we would still be able to construct $\overline{Z}$ as a variety; however, we would no longer be able to define a G-action on it, extending the G-action on Z.

8.4. Corollary. *There exist non-split elements $\alpha_n \in H^1(K_n, \mathrm{PGL}_n)$ ($n = 2, 3, \ldots$) and $\beta \in H^1(K, G_2)$ with trivial fixed point obstruction, for some finitely generated field extensions K_n/k and K/k.*

Proof. Choose α_n and β so that they are non-split and projective; cf. Section 7. $\square$

8.5. Remark. By [RY3, Theorem 4] for every prime number p there exists a non-split $\alpha \in H^1(K, \mathrm{PGL}_p)$ such that K is a purely transcendental extension of k and α has trivial fixed point obstruction. Such α are necessarily ramified and hence, cannot be projective. Thus the converse to Proposition 8.1 is false.

9. Problem 1.2 and Hilbert's 13th problem

9.1. An algebraic variant of Hilbert's 13th problem

Hilbert's 13th problem asks, loosely speaking, which continuous functions in n variables can be expressed as compositions of functions in $n - 1$ variables. In this form the problem was settled by Arnold [Ar] and Kolmogorov [Ko], who showed that any continuous function in n variables can be expressed as a composition of continuous functions in one variable and the addition function $f(x, y) = x + y$. The algebraic variant of Hilbert's 13th problem, where "continuous functions" are replaced by "algebraic functions," remains open. In modern language the problem can be stated as follows; cf. [AS,Di].

Let E/F be a finite separable field extension (or, more generally, an étale algebra) and assume that F contains a copy of the base field k. Then the *essential dimension* $\mathrm{ed}_k(E/F)$ (or simply $\mathrm{ed}(E/F)$, if the reference to k is clear from the context) is the minimal value of $\mathrm{trdeg}_k(F_0)$, where the minimum is taken over all elements $a \in E$ and over all subfields $k \subset F_0 \subset F$ such that $E = F(a)$ and F_0 contains every coefficient of the characteristic polynomial of a; cf. [BR1,BR2]. For example, if E/F is a non-trivial cyclic extension of degree n and k contains a primitive nth root of unity then $\mathrm{ed}_k(E/F) = 1$, since in this case

we can choose a so that $a^n \in F$. Note also that $\mathrm{ed}(E^\#/F) = \mathrm{ed}(E/F)$, where $E^\#$ is the normal closure of E over F; cf. [BR1, Lemma 2.3].

We will now say that E/F has level $\leqslant d$ if there exists a tower of finite field extensions

$$F = F_0 \subset F_1 \subset \cdots \subset F_r \tag{9.2}$$

such that $F \subset E \subset F_r$ and $\mathrm{ed}_k(F_i/F_{i-1}) \leqslant d$ for every $i = 1, \ldots, r$. For example, if k contains all roots of unity then every solvable extension E/F has level $\leqslant 1$ (because we can take (9.2) to be a tower of cyclic extensions). The algebraic form of Hilbert's 13th problem then asks for the smallest integer $s(n)$ such that the level of every degree n extension E/F is $\leqslant s(n)$. (Here we are assuming that the base field k is fixed throughout.) Not much is known about $s(n)$ (see [Di]); in particular, it is not known if $s(n) > 1$ for any n. It is thus natural to ask, if, perhaps, $s(n) = 1$ for all n; this equality may be viewed as an algebraic analogue of the above-mentioned theorem of Arnold and Kolmogorov; cf. [Di, p. 90]. In fact, in the absence of evidence to the contrary, one can even ask for a particularly nice tower (9.2), showing that $s(n) = 1$, namely for a tower (9.2), where F_{r-1}/F is solvable (or even abelian) and F_r/F_{r-1} has essential dimension 1. Equivalently, we have the following.

9.3. Problem. Let k be an algebraically closed field of characteristic zero, S be a finite group and K/k be a field extension. Is it true that for every $\alpha \in H^1(K, S)$ there exists (i) an abelian extension L/K such that $\mathrm{ed}(\alpha_L) \leqslant 1$? or (ii) a solvable extension L/K such that $\mathrm{ed}(\alpha_L) \leqslant 1$?

Here α_L is represented by an S-Galois algebra L'/L and $\mathrm{ed}(\alpha_L)$ denotes the essential dimension of L'/L. Equivalently, $\mathrm{ed}(\alpha_L)$ is the minimal value of $\mathrm{trdeg}_k(L_0)$ such that α_L lies in the image of the natural map $H^1(L_0, S) \to H^1(L, S)$ for some intermediate field $k \subset L_0 \subset L$. (Note, that, since the base field is assumed to be algebraically closed, $\mathrm{ed}(\alpha_L) = 0$ if and only if α_L is split.)

We do not know whether or not the assertions of Problem 9.3 are true (cf. Remark 9.6). However, using Theorem 1.1 we will show that, if true, they have some remarkable consequences.

9.4. Theorem. *Let k be an algebraically closed field of characteristic zero. and let K/k be a field extension. Denote the maximal abelian and the maximal solvable extensions of K by K_{ab} and K_{sol}, respectively.*

 (i) *If Problem 9.3(i) has an affirmative answer then $\mathrm{cd}(K_{\mathrm{ab}}) \leqslant 1$.*
(ii) *If Problem 9.3(ii) has an affirmative answer then $\mathrm{cd}(K_{\mathrm{sol}}) \leqslant 1$.*

9.5. Remark. The inequality $\mathrm{cd}(K_{\mathrm{ab}}) \leqslant 1$ is only known in a few cases; in particular, for $K = $ a number field, or $K = $ a p-adic field by class field theory and for $K = \mathbb{C}((X))((Y))$ by a theorem of Colliot-Thélène, Parimala and Ojanguren [COP, Theorem 2.2]. If it were established, it would immediately imply an affirmative answer to Problem 1.2. Another important consequence would be a conjecture of Bogomolov [Bog, Conjecture 2], which asserts that $\mathrm{cd}(K_{\mathrm{ab}}^{(p)}) \leqslant 1$, where $K^{(p)}$ is a maximal prime-to-p extension of K. On the

other hand, an affirmative answer to Problem 9.3(ii) would imply that $\mathrm{cd}_p(K(p)) \leqslant 1$, where p is a prime number and $K(p)$ is the p-closure (i.e., the maximal p-solvable extension) of K, thus giving an affirmative answer to a question of J. Königsmann; cf. [Koe, Question 5.3].

9.6. Remark. The third author would like to take this opportunity to correct a misstatement he made in [BR1, Introduction]. The identity $d'(6) = 2$, which is attributed to Abhyankar [A] at the bottom of p. 161 in [BR1], would, if true, give a negative answer to Problem 9.3(ii) for the symmetric group $G = \mathrm{S}_6$. In fact, the version of Hilbert's 13th problem considered in [A] is quite different from ours; the base extensions that are allowed there are integral ring extensions, rather than field extensions. For this reason the identity $d'(6) = 2$ does not follow from the results of [A] and, to the best of our knowledge, Problem 9.3 is still open, even in the case where S is the symmetric group S_6.

9.7. Proof of Theorem 9.4

We begin with some preliminary facts. Recall that a field F has cohomological dimension $\leqslant 1$ if and only if the Brauer group $\mathrm{Br}(F')$ is trivial for any separable finite field extension F'/F; see [Se1, Proposition II.3.5]. It will be convenient for us to work with étale K-algebras, rather than just separable field extensions of K. Recall that a K-étale algebra is a finite product $E = K_1 \times K_2 \times \cdots \times K_n$ of finite separable extensions K_i/K. The Brauer group of E is $\mathrm{Br}(E) = \bigoplus_i \mathrm{Br}(K_i)$; an element of this group is represented by an n-tuple $\mathcal{A} = (\mathcal{A}_i/K, i)_{i=1,\ldots,n}$ of central simple algebras. Note that $\mathcal{A}$ is an Azumaya algebra over E. Given a field F, we have

$$\mathrm{cd}(F) \leqslant 1 \quad \Longleftrightarrow \quad \mathrm{Br}(E) = 0 \quad \text{for any étale algebra } E/F; \tag{9.8}$$

see [Se1, Proof of Theorem III.2.2.1] or [FJ, Lemma 10.11].

9.9. Lemma. *The following are equivalent*:

(a) $cd(K_{\mathrm{ab}}) \leqslant 1$,
(b) *For any étale algebra E/K, the restriction map $\mathrm{Br}(E) \to \mathrm{Br}(E \otimes_K K_{\mathrm{ab}})$ is trivial.*

Moreover, the lemma remains true if K_{ab} is replaced by K_{sol}.

Proof. (a) $\Rightarrow$ (b). This case immediate from (9.8).
    (b) $\Rightarrow$ (a). Let B/K_{ab} be an étale algebra. There exists a finite abelian subextension K'/K of K_{ab}/K and an étale algebra B'/K' such that $B' \otimes_{K'} K_{\mathrm{ab}} = B$. We have

$$B = \varinjlim_{K' \subset L \subset K_{\mathrm{ab}}} B' \otimes_{K'} L,$$

where the limit is taken on subfields L of K_{ab} finite over K'. Consequently,

$$\mathrm{Br}(B) = \varinjlim_{K' \subset L \subset K_{\mathrm{ab}}} \mathrm{Br}(B' \otimes_{K'} L),$$

and (b) implies that $\mathrm{Br}(B) = 0$. (a) now follows from (9.8).

The proof remains unchanged if K_{ab} is replaced by K_{sol}. □

We are now ready to proceed with the proof of Theorem 9.4(i). We start with the group $G = (\mathrm{PGL}_n)^m \rtimes \mathrm{S}_m$. By Theorem 1.1(a), there exists a finite subgroup S of G such that the natural homomorphism $H^1(K, S) \to H^1(K, G)$ is surjective. The group S_m is the automorphism group of the trivial étale algebra, so by Galois descent the set $H^1(K, \mathrm{S}_m)$ classifies m-dimensional étale algebras. By [Se1, Corollary I.5.4.2], the fiber of the map $H^1(K, G) \to H^1(K, \mathrm{S}_m)$ at $[E] \in H^1(k, \mathrm{S}_m)$ is

$$H^1\big(K, {}_E\big(\mathrm{PGL}_n^m\big)\big)/{}_E(\mathrm{S}_m),$$

with ${}_E(\mathrm{PGL}_n^m)$ and ${}_E(\mathrm{S}_m)$ are the twisted groups by the étale algebra E/K. Since $G \to \mathrm{S}_m$ has a section, the map ${}_E G(K) \to {}_E(\mathrm{S}_m)(K)$ is surjective. Then ${}_E(\mathrm{S}_m)$ acts trivially on $H^1(K, {}_E(\mathrm{PGL}_n^m))$ and hence the fiber at $[E]$ is $H^1(K, {}_E(\mathrm{PGL}_n^m))$. By definition of the Weil restriction, we have ${}_E(\mathrm{PGL}_n^m) = R_{E/k}(\mathrm{PGL}_n)$. We identify $H^1(K, {}_E(\mathrm{PGL}_n^m)) = H^1(E, \mathrm{PGL}_n)$ by the Shapiro isomorphism. Thus

$$H^1(K, G) = \bigsqcup_{[E] \in H^1(K, \mathrm{S}_m)} H^1(E, PGL_n).$$

An element of $H^1(K, G)$ is then given by an Azumaya algebra $\mathcal{A}/E$ of degree n defined over a K-étale algebra E of rank m. By Theorem 1.1(a), every class $[\mathcal{A}/E]$ comes from a class $\alpha \in H^1(K, S)$.

We now apply the assertion of Problem 9.3(i) to the group S and the class α. There exists an abelian extension L/K, a k-curve C and a map $k(C) \subset L$ such that the restriction of the class α in $H^1(L, S)$ belongs to the image of $H^1(k(C), S) \to H^1(L, S)$. The commutative diagram of restriction maps

$$
\begin{array}{ccccc}
H^1(K, S) & \longrightarrow & H^1(L, S) & \longleftarrow & H^1(k(C), S) \\
\downarrow & & \downarrow & & \downarrow \\
H^1(K, G) & \longrightarrow & H^1(L, G) & \longleftarrow & H^1(k(C), G)
\end{array}
$$

shows that there exists an étale algebra $E'/k(C)$ and an Azumaya algebra $\mathcal{A}'/E'$ such that

$$E \otimes_K L \xrightarrow{\sim} E' \otimes_{k(C)} L \quad \text{and} \quad \mathcal{A}' \otimes_{E'} \big(E' \otimes_{k(C)} L\big) \xrightarrow{\sim} \big(\mathcal{A} \otimes_E (E \otimes_K L)\big).$$

Since $\mathrm{cd}(k(C)) \leqslant 1$ (see [Se1, Section II.3]), $\mathcal{A}'/E'$ is the split Azumaya algebra of rank n. We conclude that $\mathcal{A} \otimes_E (E \otimes_K L)/(E \otimes_K L)$ is the split Azumaya algebra of rank n. This shows that the map $\mathrm{Br}(E) \to \mathrm{Br}(E \otimes K_{\mathrm{ab}})$ is trivial for any étale algebra E/K. Lemma 9.9 now tells us that $\mathrm{cd}(K_{\mathrm{ab}}) \leqslant 1$. This concludes the proof of Theorem 9.4(i).

The proof of part (ii) is exactly the same, except that the field extension L/K, constructed at the beginning of previous paragraph, is now solvable, rather than abelian. $\square$

9.10. Remark. A similar argument shows that the conjecture of Bogomolov [Bog, Conjecture 2] mentioned in Remark 9.5 is a consequence of the following weaker form of Problem 9.3(i) (which is also open).

Problem 9.3′. Let k be an algebraically closed field of characteristic zero, S be a finite group, K/k be a field extension and p be a prime integer. Is it true that for every $\alpha \in H^1(K, S)$ there exists a finite extension $[K' : K]$ of degree prime to p and an abelian extension L/K' such that $\mathrm{ed}(\alpha_L) \leqslant 1$?

Acknowledgments

References

[A]   S.S. Abhyankar, Hilbert's thirteenth problem, in: Algèbre non commutative, groupes quantiques et invariants, Reims, 1995, in: Sémin. Congr., vol. 2, Soc. Math. France, Paris, 1997, pp. 1–11.

[Ar]   V.I. Arnold, On the representation of continuous functions of three variables by superposition of continuous functions of two variables, Mat. Sb. 48 (90) (1959) 3–74; English translation: Amer. Math. Soc. Transl. (2) 28 (1963) 61–147.

[AS]   V.I. Arnold, G. Shimura, Superposition of algebraic functions, in: Proc. Sympos. Pure Math., vol. 28, Amer. Math. Soc., Providence, RI, 1976, pp. 45–46.

[BP]   E. Bayer-Fluckiger, R. Parimala, Galois cohomology of the classical groups over fields of cohomological dimension $\leqslant 2$, Invent. Math. 122 (2) (1995) 195–229.

[Bog]   F.A. Bogomolov, On the structure of Galois groups of the fields of rational functions, in: K-theory and Algebraic Geometry, Connections with Quadratic Forms and Division Algebras, Santa Barbara, 1992, in: Proc. Sympos. Pure Math., vol. 58(2), Amer. Math. Soc., Providence, RI, 1995.

[BK]   F. Bogomolov, P. Katsylo, Rationality of certain quotient varieties, Mat. Sb. 126(168) (2) (1985) 584–589.

[BR1]   J. Buhler, Z. Reichstein, On the essential dimension of a finite group, Compositio Math. 106 (1997) 159–179.

[BR2]   J. Buhler, Z. Reichstein, On Tschirnhaus transformations, in: S.D. Ahlgren, et al. (Eds.), Topics in Number Theory, Kluwer Academic, Dordrecht, 1999, pp. 127–142.

[CG]   J.-L. Colliot-Thélène, Exposant et indice d'algèbres simples centrales non ramifiées, with an appendix by O. Gabber, Enseign. Math. (2002) 127–146.

[COP]   J.-L. Colliot-Thélène, M. Ojanguren, R. Parimala, Quadratic forms over fraction fields of two-dimensional Henselian rings and Brauer groups of related schemes, in: Algebra, Arithmetic and Geometry, vols. I, II, Mumbai, 2000, in: Tata Inst. Fund. Res. Stud. Math., vol. 16, Tata Inst. Fund. Res., Mumbai, 2002, pp. 185–217.

[CS]   J.-L. Colliot-Thélène, J.-J. Sansuc, The rationality problem for fields of invariants under linear algebraic groups (with special regards to the Brauer group), expanded version of the notes in: 9th Latin-American Workshop, Santiago, Chili, 1988, available at http://www.math.u-psud.fr/~colliot/Chilibib.dvi.

[Di]   J. Dixmier, Histoire du 13e probleme de Hilbert, in: Cahiers Sém. Hist. Math. Sér. 2, vol. 3, Univ. Paris VI, Paris, 1993, pp. 85–94.

[Do]   I.V. Dolgachev, Rationality of fields of invariants, in: Algebraic Geometry, Bowdoin, 1985, Brunswick, Maine, 1985, Amer. Math. Soc., Providence, RI, 1987, pp. 3–16.

[EL]   R. Elman, T.Y. Lam, Pfister forms and K-theory of fields, J. Algebra 23 (1972) 181–213.

[EM]   S. Endo, T. Miyata, Invariants of finite abelian groups, J. Math. Soc. Japan 25 (1973) 7–26.

[FJ]   M.D. Fried, M. Jarden, Field Arithmetic, Springer-Verlag, Berlin, 1986.

[Ga]   L.Y. Galitskii, On the existence of Galois sections, in: Lie Groups, Their Discrete Subgroups and Invariant Theory, in: Adv. Soviet Math., vol. 8, Amer. Math. Soc., Providence, RI, 1992, pp. 65–68.

[GMS]   S. Garibaldi, A. Merkurjev, J.-P. Serre, Cohomological invariants in Galois cohomology, in: University Lecture Ser., vol. 28, Amer. Math. Soc., Providence, RI, 2003.

[Gi]   P. Gille, Cohomologie galoisienne des groupes quasi-déployés sur des corps de dimension cohomologique $\leqslant 2$, Compositio Math. 125 (3) (2001) 283–325.

[GM]   A. Grothendieck, J.P. Murre, The Tame Fundamental Group of a Formal Neighbourhood of a Divisor with Normal Crossings on a Scheme, Lecture Notes in Math., vol. 208, Springer-Verlag, Berlin, 1971.

[Ka]   P.I. Katsylo, Rationality of the orbit spaces of irreducible representations of the group SL_2, Izv. Acad. Nauk SSSR Ser. Mat. 47 (1983) 26–36; English translation: Math. USSR-Izvestya 22 (1) (1984) 23–32.

[Ko]   A.N. Kolmogorov, On representation of continuous functions of many variables by superposition of continuous functions of one variable and addition, Dok. Akad. Nauk 114 (5) (1957) 953–956; English translation: Amer. Math. Soc. Transl. (2) 28 (1963) 55–59.

[Koe]   J. Königsmann, Elementary characterization of fields by their absolute Galois groups, Habilitationsschrift, Konstanz, 1998.

[L]   H.W. Lenstra Jr., Rational functions invariant under a finite abelian group, Invent. Math. 25 (1974) 299–325.

[Mu]   D. Mumford, The Red Book of Varieties and Schemes, Lecture Notes in Math., vol. 1358, Springer-Verlag, Berlin, 1988.

[PR]   V. Platonov, A. Rapinchuk, Algebraic Groups and Number Theory, Academic Press, New York, 1994.

[Po]   V.L. Popov, Sections in invariant theory, in: The Sophus Lie Memorial Conference, Oslo, 1992, Scand. Univ. Press, Oslo, 1994, pp. 315–361.

[PV]   V.L. Popov, E.B. Vinberg, Invariant Theory, in: Encyclopaedia Math. Sci., vol. 55, A.N. Parshin, I.R. Shafarevich (Eds.), Algebraic Geometry IV, Springer–Verlag, Berlin, 1994.

[Re]   Z. Reichstein, On the notion of essential dimension for algebraic groups, Transform. Groups 5 (3) (2000) 265–304.

[RY1]   Z. Reichstein, B. Youssin, Essential dimension of algebraic groups and a resolution theorem for G-varieties, Canad. J. Math. 52 (5) (2000) 1018–1056. With an appendix by J. Kollár and E. Szabó.

[RY2]   Z. Reichstein, B. Youssin, Splitting fields of G-varieties, Pacific J. Math. 200 (1) (2001) 207–249.

[RY3]   Z. Reichstein, B. Youssin, A non-split torsor with trivial fixed point obstruction, J. Algebra 263 (2) (2003) 255–261.

[Sa]   J.-J. Sansuc, Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres, J. Reine Angew. Math. 327 (1981) 12–88.

[Se1]   J.-P. Serre, Galois Cohomology, Springer-Verlag, 1997.

[Se2]   J.-P. Serre, Cohomologie galoisienne: progrès et problèmes, in: Séminaire Bourbaki, vol. 1993/94, Exp. 775–789, Astérisque 227 (1995) 229–257.

[Sh]   I.R. Shafarevich, Basic Algebraic Geometry, vol. 1, second ed., Springer-Verlag, 1994.

[Si]   J.H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, New York, 1986.

[Sp]   A. Speiser, Zahlentheoretische Sätze aus der Gruppentheorie, Math. Z. 5 (1919) 1–6.

[T1]   J. Tits, Classification of algebraic semisimple groups, in: A. Borel, G. Mostow (Eds.), Algebraic Groups and Discontinuous Subgroups, in: Proc. Sympos. Pure Math., vol. 9, Amer. Math. Soc., Providence, RI, 1966, pp. 33–62.

[T2]   J. Tits, Résumé de cours au Collège de France 1991–92, Annuaire du Collège de France, 1992.